Healthfully

Information Security Policies and Procedures

Revision History

REVISION	DESCRIPTION OF CHANGE	UPDATE DATE	UPDATE BY	UPDATE APPROVAL	APPROVAL DATE
v1.0	Original	8/9/2019	Kristen Hostetter		
v1.1	Document revision	8/17/2020	Kristen Hostetter		
v1.2	Document revision	2/19/2021	Kristen Hostetter		
v2.0	Overall formatting change to track executive management approval and general operations review	12/5/2022	Danya Gayle	Kristen Hostetter	12/9/2022
V2.1	Review, formatting update	8/3/2023	Kristen Hostetter		8/3/2023

Contents

1 Corporate Information Security Policy - Summary

The purpose of this document is to inform Healthfully Inc.'s ("Healthfully") Associates (employees, contractors, vendors, and any other person using or accessing Healthfully information or systems) about the Company's policies for the use of the internet and Intranet hereafter referred to as "the Services" via the company network. The policies are designed to minimize potential risks associated with connecting the services without unduly limiting the potential benefits offered by timely access to information to serve our client's needs.

General Policy
The network is intended for business use only. It is provided to Healthfully Associates to increase productivity. Viewing, downloading, copying, sending, or processing information outside the scope of company business is strictly prohibited. The Company provides the Services through its network to Associates as a business privilege which can be revoked by the Company at any time, with or without notice.

All transactions conducted via the Company network could be perceived as authorized Company activities. Therefore, the content accessed via the Services must comply with Healthfully standards and Healthfully's Acceptable Use Policy for Electronic Communications (located in Exhibit A herein) should exclude obscene, harassing, or otherwise offensive language, pictures, drawings, graphics, or other materials.

Publishing on Behalf of the Company
Some Associates will have sufficient access to place material on the Company's website(s) or Intranet. Those Associates are, in effect, publishing on behalf of the Company and must observe all applicable standards, policies, and regulations. They will be accountable for all information regarding the Company business or publications posted for public access, including information obtained through hyperlinks to external information. Any software posted on a Company site must comply with U.S. laws regulating encryption and copyrights.

Copying/Downloading
There is material on the Internet which is protected by copyright laws. Associates must refrain from violating those laws by copying or making available copies of protected works. Associates are responsible for observing copyright and licensing agreements and must follow the appropriate procurement process before downloading any materials for which a fee is requested. Downloading software from the Internet to a computer on the Healthfully network also requires approval from the IT department, to ensure compliance with enterprise-wide standards.

Other Third-Party Rights
Associates using the Services are prohibited from sending or posting messages that contain abusive or objectionable language, that defame or libel others, or that infringe on the privacy rights of others. Also prohibited is transmission or posting of messages intended or likely to

result in the loss of the recipient's work or systems, including but not limited to dissemination of high volumes of unsolicited E-mail ("spam").

Network Security
Use of the Services in a manner which could compromise the security and integrity of the network is prohibited. This includes, but is not limited to, knowingly allowing intruders or viruses to penetrate the network. The company maintains a firewall designed to protect the network from such potential dangers and to secure information. Anyone using a computer attached to the network must access the Internet through this firewall, not directly through a modem or other device.

Compliance
Healthfully retains the right to monitor and review use of the Services, including E-mail, by its Associates. The IT Department may conduct random audits of Internet/Intranet use. The purpose of these audits is to ensure compliance with this policy statement. Associates using the Services waive any right to privacy and consent to access and disclosure of usage, and communications, by the Company. Failure to adhere to these guidelines may result in disciplinary action up to and including termination.

Periodic Review of Risks
Critical processes that are implemented at Healthfully will undergo a comprehensive risk assessment to identify critical information assets, threats to those assets, and effectiveness of risk controls. The risk assessment will review risks to the entire process and not limited to specific IT systems. The risk assessment will be updated on an annual basis. As threats, operation environments and systems architecture change, Information Security personnel will create and update risk assessments to ensure that new risks are mitigated prior to making changes to the infrastructure, policies, and procedures. Information Security personnel will review risks on an annual basis.

Consistency with Laws and Regulations
Senior management reviews and approves the security policy annually and ensures consistency with applicable laws and regulations (e.g., HIPAA Security Rule), defined commitments, service level agreements, and other contractual requirements.

Policy Exemptions
The policy applies to all Healthfully employees, contractors, vendors, and any other person using or accessing Healthfully information or systems. Exemptions to this policy must be documented and approved by the CEO with the HIPAA Security Officer or designated representatives.

Training
Each new hire will complete training to include an overview of Healthfully’s security policies and procedures. The policies will include end user acceptable use as well as data handling and

disposal training in addition to other security safeguards. New employees will receive training as well for the use of the systems and applications required to perform their job function.

All staff will be trained on security, compliance, and operating procedures to effectively use Healthfully information systems and applications required while performing their job duties. Healthfully staff will receive annual training on security awareness.

HIPAA Record Retention
Healthfully maintains formal records of policies, procedures, actions, activities, and assessments as required by the HIPAA Security Rule and retains HIPAA-required documentation for the time period required (6 years). The following records should be retained, among others:

- Policies and procedures in effect during the retention period
- Security risk analyses
- Incident documentation for any privacy and security incidents that occur
- Breach notification documentation for any breaches that occur
- Employee sanction documentation
- Complaint and resolution documentation
- Regulatory compliance correspondence and assessment reports
- Business associate agreements with service providers and contractors
- Physical security maintenance records
- Information systems activity reviews, decisions made, and investigations conducted
- Log records pertaining to views and updates of ePHI
- Contingency plans in effect during the retention period
- Contingency plan tests
- Records of the movements of hardware and electronic media used to store ePHI, including the receipt of any new hardware or electronic media storing ePHI. This record should contain, at a minimum, the name of the person responsible for the item, the location of the item, and any movement of the item.

2 Purpose

To be effective, information security must be a team effort involving the participation and support of every Healthfully Associate who deals with information and/or information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users as well as the steps they must take to help protect Healthfully's information and information systems. This document describes ways to prevent and respond to a variety of threats including unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of Healthfully's information.

Information is essential input to all the work that Healthfully performs. As a result, information security has become a critical factor in the production of Healthfully's products and services. In

recognition of this fact, an Information Security Officer acts as Healthfully's focal point for all information security issues. Specific questions about the policies described here can be directed to the Information Security Officer. In some cases, questions will be answered via the glossary of terms at the end of this policy statement.

Training is an important part of ensuring the confidentiality, integrity and availability for client and company information. In order to minimize possible security risks, all company staff will be trained in their specific responsibilities under the information security program.

3 Scope

This policy statement applies to all Associates, contractors, consultants, temporaries, and other workers at Healthfully, Inc., including those workers affiliated with third parties who access Healthfully computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals.

This policy statement applies to all computer and data communication systems owned by and/or administered by Healthfully. The document covers only information handled via computers and/or networks. Although the document includes mention of other manifestations such as voice and paper, it does not directly address the security of information in these forms.

4 Roles and Responsibilities

The CEO along with the CTO and the Security Officer are responsible for considering any and all impacts to policies and procedures when changes in the existing systems may affect security.

Information Security personnel facilitate fulfillment of the request for access by Managers. Responsibilities include assessing the risks electronic communication use presents to Healthfully consulting with management on risks or recommending the necessary action to protect corporate assets and systems. With management concurrence, Information Security will implement or assist with the implementation of appropriate security monitoring and protection tools, systems and techniques.

Information Security personnel will remain vigilant for new threats that may impact Healthfully systems and client data.

Information Security may, as deemed necessary by management, review any and all files, messages, and systems (including voicemail and e-mail) to determine compliance with policy and to assist in protecting the corporation assets.

Information Systems is responsible for providing the capacity and ability to connect to the electronic communication. This includes the responsibility for actively monitoring system performance to identify instances where excessive use of resources may degrade performance of production systems, assist in identifying risks, recommend solutions to management and Information Security and responsible for taking action to resolve performance issues when identified.

Managers determine Associates' need for access and provide authorization to Information Security to establish the necessary access. This includes ensuring Associates understand the expectations for electronic communication use and ensuring Associates know how to use the electronic communication productively. Managers are also responsible for monitoring their Associates' use, identifying instances of improper or unproductive use of Associates' time and/or corporate system resources. This includes taking action as deemed appropriate for the improper use and reporting this information to Information Security.

Custodians are in physical or logical possession of either Healthfully information or information that has been entrusted to the Company. While Information Technology organization staff members clearly are Custodians, distributed multi-user system administrators are also Custodians. In some cases, multiple Custodians may exist. Whenever information is maintained only on a personal computer, the User is necessarily also the Custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

Users are responsible for familiarizing themselves with and complying with all Healthfully policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Managers of the involved information.

Each new hire granted access to client information and other classified Healthfully data will undergo a background check. Any past activity that would subject sensitive systems and data to risk due to an employee's past behavior will be cause to terminate.

Termination Processes:
The following standards will be followed upon the resignation of an employee, member of Management, IT Staff and third-party vendors.

1. IT will remove employee access from any and all systems or applications that processed or stored sensitive information on the employee's last working day.
2. Remote connectivity will be removed.
3. Card Keys issued to the employee will be returned.

4. Following a termination an employee will not be provided access to their desk or office – any such access, if provided, must be limited and supervised.

5 General Disclosure Policy

There are three types of information within Healthfully, Inc. Information which has been designated by its Owner as PUBLIC can be disclosed to anyone, both inside and outside of Healthfully, without formal management approval. Information which has been designated by its Owner as INTERNAL may be disclosed to any Healthfully worker. Information which has been designated by its Owner as CONFIDENTIAL may only be disclosed to persons who have been specifically authorized to receive the information. Authorization will be granted by the information's Owner consistent with the need-to-know. When the term "need-to-know" is used it means that the recipient requires access to perform ordinary job duties, or to complete a special project which has been authorized by Healthfully management.

Information which does not have either a PUBLIC or a CONFIDENTIAL designation must be treated as though it were INTERNAL until its Owner designates a fitting classification. In addition, information belonging to third parties--that has been entrusted to Healthfully--must be treated as though it were CONFIDENTIAL unless a contract or some other written agreement specifies otherwise.

To classify a document as CONFIDENTIAL, a specific reason must be determined by the Owner. Reasons include information of a sensitive nature or the determination that disclosure of such information would result business interruption or negatively affect operations. Information designated as CONFIDENTIAL will remain so classified until specifically declassified by the Owner or another Healthfully manager to whom these ownership responsibilities were delegated. The only exception involves information which has been specifically marked to become PUBLIC or INTERNAL as of a certain date

Disclosure of CONFIDENTIAL information to anyone (whether a Healthfully employee or not) is prohibited unless this access has been previously authorized by the information Owner. All recipients who are not Healthfully Associates must sign a confidentiality agreement prior to taking possession of CONFIDENTIAL information. CONFIDENTIAL information Custodians must verify the existence of such a signed confidentiality agreement prior to disclosure to non-Associates.

6 Confidential Information Marking

Every paper document that has been designated as CONFIDENTIAL must have the designation appear on the top and bottom of every page. Bound paper documents must be marked on the front and back covers in the same manner. Electronic versions of documents must display the

CONFIDENTIAL marking on the first screen shown to the user. All hardcopy computer output designated as CONFIDENTIAL must conform to paper document marking requirements. All computer-readable storage media containing CONFIDENTIAL information must have a CONFIDENTIAL designation on its external label.

7 Confidential Information Handling, Storage, Reproduction, Transport, and Destruction

Users handling CONFIDENTIAL information must be vigilant to make sure the information is not inadvertently disclosed to people who do not have a need-to-know. Users must cover CONFIDENTIAL information on their desks or working areas when unauthorized persons are in the immediate area. Likewise, users must enable a screen saver, log-off, or take similar actions if unauthorized persons are in a position to see the screen of their computer terminals. All Healthfully computers storing CONFIDENTIAL information must have an installed and enabled password-based access control package.

When not in use, or when not under direct and continuous visual supervision, CONFIDENTIAL information must be stored in a secure container such as a locked cabinet or a locked desk. CONFIDENTIAL information which has been encrypted according to Healthfully approved methods need not be stored in a secure container. CONFIDENTIAL information which cannot be under direct and continuous visual supervision--such as information stored on a portable computer hard disk drive--must be encrypted with Healthfully approved methods.

Reproduction of CONFIDENTIAL information, including printing additional copies via a computer printer, is not permitted unless specifically authorized by its Owner. Likewise, extracts, summaries, translations, or derivatives of CONFIDENTIAL information may not be made unless the information Owner has previously approved. Custodians may make back-up of CONFIDENTIAL copies without specific Owner approval.

Physical transport of CONFIDENTIAL information requires the use of a trusted courier such internal mail staff, the US Postal Service, UPS, or Federal Express. All CONFIDENTIAL information sent via such couriers must be enclosed in an opaque and sealed envelope. If CONFIDENTIAL information is stored on computer-readable storage media such as a floppy disk it must be encrypted when sent by courier. Likewise, whenever CONFIDENTIAL information is sent over external computer networks, such as the Internet, it must be in encrypted form.

When CONFIDENTIAL information is no longer required, and when legal or regulatory requirements for its retention no longer apply, it must be destroyed according to approved methods. Disposal in trashcans or recycling bins is prohibited. CONFIDENTIAL information must be shredded if in paper form. CONFIDENTIAL information residing on hardware that is no

longer required will be placed into a locked bin that will be scheduled for destruction on a periodic basis. The date of destruction will be recorded and logged.

8 System Access Control

8.1 Passwords

Healthfully requires the use of strong passwords. Users are required to follow the below requirements and suggestions when creating passwords.

Difficult-to-Guess Passwords
Passwords are an essential component of Healthfully's computer and network security systems. To ensure that these systems do the job they were intended to do, users must choose passwords that are difficult-to-guess. This means that passwords must NOT be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used.

Repeated Password Patterns
Users must not construct passwords with a basic sequence of characters that is then partially changed based on the date or some other predictable factor. For example, users must NOT employ passwords like "X34JAN" in January, "X34FEB" in February, etc. Additionally, users must not construct passwords that are identical or substantially similar to passwords they have previously employed.

Password Constraints
To make guessing more difficult, passwords must also be at least eight characters long with password complexity rule (using numbers, upper case letters and special characters). To ensure that a compromised password is not misused on a long-term basis, passwords must also be changed every 45 days or at more frequent intervals.

Password Storage
Passwords must never be stored in readable form. This includes but is not limited to within batch files, automatic log-in scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them such as text files saved on network drives or desktops. Similarly, passwords must not be written down in notebooks or on sticky-notes even if stored in a drawer or left in a place where unauthorized persons might discover them. Aside from initial password assignment and password reset situations, if there is reason to believe that a password has been disclosed to someone other than the authorized user, the password must be immediately changed.

Sharing Passwords
Regardless of the circumstances, passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions that the other party takes with the disclosed password.

8.2 Access Control System Design

Internal Network Connections
All Healthfully computers which are permanently or intermittently connected to internal computer networks must have an approved password-based access control system. This requirement includes computers with direct connections to the Corporate Data Center as well as to Healthfully's wide area network. Regardless of the network connections, all computers handling or which could possibly access CONFIDENTIAL information must also employ approved password-based access control systems.

External Network Connections
All inbound connections to Healthfully computers from external networks must be protected with an approved access control system and utilize a communication method that protects data in transit (e.g., HTTPS, SSL, TLS, FTPS).

Lock Screen and Automatic Logout
All users with computers must use screen savers that blank the screen and require a password to resume work. Screen savers ensure that unauthorized persons are not able to use computers or view the data stored thereon while authorized users are away from their desks. Multi-user Healthfully systems must employ automatic logout controls that terminate a user's session after a certain period of inactivity.

Unique UserIDs and Passwords
All access control systems must utilize userIDs and passwords unique to each user, as well as user privilege restriction mechanisms. Unique userIDs and passwords are required to protect users from unwarranted suspicion associated with computer crime and abuse. Unique userIDs and passwords also help maintain the integrity of Healthfully information by reducing unexplained errors and omissions. Additionally, the dissemination of CONFIDENTIAL information cannot be tracked unless unique userIDs and passwords are employed.

Anonymous UserIDs
With the exception of Internet web sites, or other systems where all regular users are intended to be anonymous, users are prohibited from logging into any Healthfully system or network anonymously. Guest accounts are strictly prohibited.

Vendor-Provided Passwords

To prevent unauthorized access by unknown persons, all vendor-supplied default passwords must be changed before any computer or communications system is used for Healthfully production application processing. This policy applies to passwords associated with end users, as well as systems administrators and other privileged users.

File Permissions

On those systems which allow users to define their own file access privileges, users must not automatically grant others on the system privileges to read, write, or execute their files. For example, on UNIX systems, users must not grant default "world" read/write/execute privileges to other users. Users are permitted to reset permissions on a file-by-file basis, but all such changes will be logged.

Access Requests

Requests for new userIDs and changed privileges must be in writing (ticket request) and approved by the user's manager before a Systems Administrator fulfills these requests. Users must clearly state why the changes in privileges are necessary and how this change pertains to their job. Individuals who are not Healthfully Associates must not be granted a userID or otherwise be given privileges to use Healthfully computers or communications systems unless the advance written approval of a Department Manager has first been obtained.

Access Denial

All userIDs which have been inactive for 30 or more days will automatically have the associated privileges revoked. System privileges will be reestablished only after the involved users obtain management written approval for their access requests. When users are transferred to a different job, their system privileges will be changed to reflect their new job duties. In addition to promptly reporting changes in the status of workers, every six months the Information Security team will review the suitability of user system privileges. In response to feedback from management, Systems Administrators will revoke any privileges no longer needed by users. Healthfully management reserves the right to revoke the system privileges of any user at any time.

Prohibited Activities

Conduct that interferes with the normal and proper operation of Healthfully information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted. Users must not test or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by Executive Management. Incidents involving unapproved system hacking, password cracking, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful and will be considered serious violations of Healthfully policy. Likewise, short-cuts bypassing systems security measures, as well as pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

9 Establishment of Access Paths

Network Changes
Changes to Healthfully internal networks include loading new communications software, changing network addresses, reconfiguring routers, adding inbound connectivity, and the like. With the exception of emergency situations, all changes to Healthfully computer networks must be: (a) documented in a work order request, and (b) approved in advance by the IT Department. All emergency changes to Healthfully networks must only be made by persons who are authorized by the IT Department. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to "workers" as defined in the Scope section of this policy, but also to vendor personnel.

New Systems Setup
Workers must NOT establish electronic local area networks, connections to local area networks, or other multi-user systems for communicating information without the specific approval of the IT Department. Likewise, new types of real-time connections between two or more in-house computer systems must not be established unless such approval has first been obtained. This policy helps to ensure that all Healthfully systems have the controls needed to protect other network-connected systems. The actual security of a network-connected computer is not just a function of that machine's security mechanisms, it is also a function of all other connected systems.

10 Monitoring and Reporting

Logs for all system components will be reviewed at a minimum on a monthly basis. Log reviews will include those servers that perform security functions such as authenticating users. Logging must be enabled in order to establish a sufficient audit trail for all access to sensitive data. Logging will be performed at the application level as well.

Automated audit trails must be implemented to reconstruct the following events, for all system components:

- User access to system components, especially for users with administrative privileges
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs

Audit trails will log the following:

- User Identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, system component, or resource

Audit trails will be secured so they cannot be altered in any way:

- Limit viewing of audit trails to those with a job-related need.
- Protect audit trail files from unauthorized modifications.
- Promptly back-up audit trail files to a centralized log server or media that is difficult to alter.

Event logging will be consolidated to monitor and analyze compliance to company security policies.

Access Monitoring

- Firewall and server logs will be reviewed regularly for anomalies.
- Record and report failed log-in attempts on a regular basis.
- Provide immediate notification to the network administrator to respond to potential attacks profiled by failed logon attempts.
- Log all attempts to gain entry onto the Healthfully network or critical applications. The following attempted access activities will be monitored and recorded:
    - Logons
    - Failed Logon attempts
    - Failed file access attempts
    - All privileged user actions
- Provide an exception report to the Information Security Officer for all access control violations on a regular basis.
- Log reviews must include those servers that perform security functions such as authentication servers.

11 Internet Connections and Electronic Mail

Use of the Services is encouraged where it is suitable for business purposes, supports the goals and objectives of the organization, and is consistent with User's job responsibilities. The Services are valuable corporate resources and must not be used for personal gain including solicitation of non-company business, advancement of individual views, or illegal activity. Disciplinary action, including discharge, may result from failure to adhere to this policy.

All information posted on the Internet representing Healthfully, Inc. or its subsidiaries must be approved by the appropriate corporate legal department, consistent with the Company's policy for communicating information to the public. Users are prohibited from creating unauthorized Web pages, information sites, or posting statements representing the Company on the Internet or Intranet. Only management may send broadcast messages to all e-mail Users within one or more of the Healthfully companies.

The Services must not be used for illegal activities, such as harassing other users, accessing or distributing threatening or obscene material, the intentional spread of computer viruses or other destructive information, malicious service disruption, unauthorized attempts to break into any computer system or use resources or access or destroy data belonging to the company or any other organization or individual, or unauthorized use or retrieval or distribution of copyrighted material. Users assume personal liability for any and all violations committed while using the Services.

Access to the Services must be approved by the User's management. Only company-approved software may be used when connecting to the Internet. Before access to the Services will be granted, the User is required to acknowledge receipt of this policy and sign a statement of intended compliance. Account Ids and passwords for the Services are strictly for the use of the registered User and should not be shared or made accessible to others.

Workers must not send logins or passwords, protected health information, payments information, or any CONFIDENTIAL information via Internet electronic mail if it is in readable (unencrypted) form.

Downloading software and files from non-Healthfully sources via the Internet (or any other public network) is strictly prohibited.

Healthfully is committed to respecting the rights of its Associates, including their reasonable expectation of privacy. Healthfully also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas.

Senior management is strictly accountable to Healthfully’s stakeholders for the enforcement of this policy. Users and their managers are strictly accountable for the accuracy and appropriateness of links and information available from the User's Internet or Intranet sites.

12 Computer Viruses

A computer virus is an unauthorized program that replicates itself, attaches itself to other programs, and spreads onto various data storage media and/or across a network. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers.

To assure continued uninterrupted service for both computers and networks, all computer users must keep current versions of approved virus screening software enabled on their computers. This screening software must be used to scan all software coming from either third parties or other Healthfully groups; the scanning must take place before the new software is executed. Users must not bypass scanning processes that could arrest the transmission of computer viruses.

If users suspect infection by a computer virus, they must immediately stop using the involved computer and call the IT systems administrators. Media with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves; Healthfully staff with expertise in virus eradication or qualified consultants will be called in to complete this complex task in a manner that minimizes both data destruction and system downtime.

13 Application Development

All software developed and intended to process critical, valuable, or CONFIDENTIAL information, must have a written formal specification. This specification must include discussion of both security risks and controls (including access control systems and contingency plans) and discussion of the potential privacy impact when new processes involving personal information are implemented, and when changes are made to such processes. The specification must be part of an agreement between the involved information Owner and the system developer.

Before being used for production processing new or substantially changed application systems must have received written approval from the VP of Development for the controls to be employed.

All computer and communications systems used for production processing at Healthfully must employ a documented change control process which is used to ensure that only authorized changes are made. This change control procedure must be used for all significant changes to software, hardware, communications links, and related procedures.

All software development and software maintenance activities performed by staff must subscribe to Healthfully IT Department policies, standards, procedures, and other systems development

conventions. Among other things, these conventions include the proper testing, training, and documentation.

The use of personal information in process and system development and test is prohibited unless such information is anonymized or otherwise protected in accordance with Healthfully's privacy policies and procedures.

14 Encryption

Encryption is a process for concealing information so that unauthorized parties cannot examine or use it. When CONFIDENTIAL information is transmitted over any communication network provided by an organization outside Healthfully, it must be sent in encrypted form. Information which has been entrusted to Healthfully by a third party must also be encrypted when sent over external network systems.

Similarly, whenever CONFIDENTIAL information is not being actively used, it must be stored in encrypted form. This means that when CONFIDENTIAL information is stored or transported in computer-readable storage media, it must be in encrypted form or password protected.

Encryption of information at rest (in storage) or in transit (on a network) must be achieved via commercially available products approved by the IT Department. All encryption algorithms (methods), modes of operation (implementation details), and key management systems (ways to manage secret parameters) must be consistent with internal standards issued by the Information Security Department.

Encryption keys used for Healthfully information are always classified as CONFIDENTIAL information. Access to such keys must be strictly limited to those who have a need-to-know. Unless the approval from the IT Department is first obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or third parties. Likewise, encryption keys must always be encrypted when sent over a network.

15 Portable Computers

Workers in the possession of portable, laptop, notebook, and other transportable computers containing CONFIDENTIAL information must not leave these computers unattended at any time unless the information is stored in encrypted form.

Whenever CONFIDENTIAL information is written to an external storage media, the storage media must be suitably marked CONFIDENTIAL. When not in use, this media must be stored in a locked safe, locked furniture, or a similarly secured location.

The security of Healthfully property at an alternative worksite is just as important as it is at Healthfully offices. At alternative worksites, reasonable precautions must be taken to protect Healthfully hardware, software, and information from theft, damage, and misuse. To this end, Healthfully maintains the right to conduct inspections of telecommuter offices with one or more days advance notice.

CONFIDENTIAL information may not be removed from Healthfully premises unless there has been prior approval from the information's Owner. This policy includes CONFIDENTIAL information stored on portable computer hard disks, external storage media, hard-copy output, paper memos, and the like. An exception is made for authorized off-site back-ups.

Workers must not bring their own computers, computer peripherals, or computer software into Healthfully facilities or link to the Healthfully network. This includes portables, laptops, and other such equipment.

16 Remote Printing

Printers must not be left unintended if CONFIDENTIAL information is being printed or will soon be printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted only if the area surrounding a printer is physically protected such that persons who are not authorized to see the material being printed may not enter.

17 Privacy and Personal Use

Unless contractual agreements dictate otherwise, all information stored on or transmitted by Healthfully computer and communications systems is Healthfully property. To properly protect and manage this property, Healthfully management reserves the right to examine all information stored in or transmitted by these systems. Workers should have no expectation of privacy associated with the information they store in or send through these systems. Because this information is Healthfully property, users must not put it to uses that have not been explicitly approved by the information Owner.

Workers may be subject to electronic monitoring while on Healthfully premises and while using Healthfully information systems. This monitoring is used to measure workers performance as well as to protect worker personal property, worker personal safety, and Healthfully property.

At any time and without prior notice, Healthfully management reserves the right to examine archived electronic mail, personal file directories, hard disk drive files, and other information stored on Healthfully information systems. This examination is performed to assure compliance with internal policies, support the performance of internal investigations, and assist with the

management of Healthfully information systems. Healthfully retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Healthfully's code of conduct prohibits workers from using Healthfully time, facilities, equipment or supplies for private gain or advantage. Accordingly, Healthfully computer and communications systems must be used for business purposes only. Personal use is allowed only by special permission of a local program manager.

18 Software Coping

Healthfully provides a sufficient number of licensed copies of software such that workers can get their work done in an expedient and effective manner. Healthfully management must make appropriate arrangements with the involved vendors for additional licensed copies, if and when additional copies are needed for business activities.

Users must not copy software provided by Healthfully to any storage media, transfer such software to another computer, or disclose such software to outside parties without written permission from the Executive Officers. Ordinary back-up copies are an authorized exception to this policy.

Unless specifically authorized by the IT Department, Healthfully workers must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those which defeat software copy-protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

19 Physical Security of Servers and Network

All Healthfully computer and network equipment must be physically secured with anti-theft devices if located in an open office environment. Local area network hardware must be placed in locked cabinets, locked closets, or locked computer rooms.

- All development, test, and production infrastructure (servers, network equipment, redundant and disaster recovery solutions) are hosted at a SOC-2 compliant data center
- All other network equipment is either protected in a locked cage/cabinet, a locked closet or a locked computer room depending on office location.

The office building is accessible M-F 8:00 AM to 5:00 PM and is secured via key card and an alarm system. After hours, weekends and holidays the office building is accessible with arranged security escort. Healthfully office suites are secured via deadbolt. The deadbolt lock key is only issued to Healthfully management and two Associates. Healthfully network systems kept in a

locked server room or locked closet are only accessible to approved personnel. Visitors and contractors to our office suite must knock on our doors and must sign-in.

Healthfully datacenter is owned and operated by Amazon. We employ Amazon Web Services (AWS) cloud service computing environment to process, store and transmit the protected health information (PHI) of our customers. AWS services and data centers have multiple layers of operational and physical security to ensure the integrity and safety of data. Their infrastructure and platforms receive industry-recognized certifications such as: ISO 27001, FedRAMP and Service Organization Control (SOC) Reports. AWS aligns their HIPAA risk management program with FedRAMP and NIST 800-53, higher security standards that map to the HIPAA Security Rule.

Access to infrastructure during an outage or designated emergency is outlined in the 'Healthfully Business Continuity Plan'.

Healthfully maintains a log and supporting work orders, invoices, etc. for repairs and modifications to the physical components of a facility which are related to security.

20 Handling Security Information

Information about security measures for Healthfully computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless the permission of the IT Department has first been obtained. For example, publishing system access information is prohibited. Nonetheless, public disclosure of electronic mail addresses is permissible.

21 Violations

Healthfully workers who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.

All suspected policy violations, system intrusions, virus infestations, and other conditions which might jeopardize Healthfully information or Healthfully information systems must be immediately reported to the IT Department.

22 Security Incidents

Healthfully maintains and Incident Response Plan, which is documented in the 'Healthfully Incident Response Plan'.

Glossary

Access control: A software system to restrict the activities of users and processes based on the need-to-know.

Algorithm: A mathematical process for performing a certain calculation; in the information security field, generally used to describe an encryption process.

Booting: The process of initializing a computer system from a turned-off state.

Compliance statement: A document used to obtain a promise from a computer user that the user will abide by system policies and procedures.

Confidential information: A designation for information, the disclosure of which is expected to damage Healthfully, business partners, customers, or other involved parties.

Critical information: Any information essential to Healthfully's activities, the destruction, modification, or unavailability of which would cause serious disruption to Healthfully's mission.

Decompression: A computer process by which compacted data is expanded to its full and normal size so that it can be used.

Decryption: The mathematical process by which an encrypted message is rendered readable or usable (reverses the encryption process); also called decipherment.

Default classification: The sensitivity classification (confidential) applied to information when an Owner has not yet specifically designated a classification.

Default file permission: Access control file privileges (read, write, execute, etc.) granted to computer users without further involvement of either a security administrator or users.

Default password: An initial password provided by a computer vendor when hardware/software is first delivered.

Digital signature: A sequence of bits which accompanies a message that is generated via encryption; such a bit sequence shows that a message (a) was sent by an identified person, and (b) is free from modification or tampering.

Encryption: A mathematical process involving data coding to achieve confidentiality as well as other security objectives; also called encipherment.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

End-user: A user who employs computers to support Healthfully activities, who is acting as the source or destination of information flowing through a computer system.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security test (such as providing a dynamic password).

Isolated computer: A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.

Log-in script: A set of stored commands which can log a user into a computer automatically.

Multi-user computer system: Any computer which can support more than one user simultaneously.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password reset: The assignment of another (temporary) password when a user forgets or loses his/her password.

Password-based access control: Software which relies on passwords as the primary mechanism to control system privileges and logging activities.

Password: Any secret string of characters used to identify a computer user or process.

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user-ID: A user-ID which has been granted the ability to perform special activities, such as shut down a multi-user system.

Revoke privileges: A process whereby the system access permissions associated with a specific user are removed.

Router: A device that interconnects networks; used in some instances to provide access control and message routing services.

Screen saver: A computer program that automatically blanks the screen of a computer monitor after a certain period of no activity.

Sensitive information: Any information, the disclosure of which could damage Healthfully, business partners, customers, or other third parties.

Shared password: A password known by and/or used by more than one individual.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Special system privilege: Access system privileges allowing the involved user or process to perform activities which are not normally granted to other users.

Systems administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

UserIDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Healthfully or another party.

Virus screening software: Commercially available software that searches for certain bit patterns or other evidence of computer virus infection.

Exhibit A

Healthfully Acceptable Use Policy for Electronic Communications Services, Equipment and Data

Introduction

Healthfully recognizes that use of the Internet, Healthfully's computer network and other electronic communications and data resources has many benefits for Healthfully's clients, employees and our Associates. The Internet and e-mail make communication more efficient and effective. Unacceptable usage of the Internet, Healthfully's computer network or other electronic communications and data resources can harm Healthfully and its relationship with clients.

Healthfully provides its employees (whether full time, part-time or temporary), consultants and other workers for Healthfully ("Service Users") with access to Healthfully's computer network, computer hardware and software, data, databases, storage media, Internet, E-mail, mobile telephones, voice mail, and other current and future computer, electronic communications and data resources, whether owned, leased by or contracted to Healthfully ("Electronic Services") so that they may be used for Healthfully's lawful business purposes ("Business Use"). Healthfully recognizes that there may also be periodic need to utilize these Electronic Services (except the data and databases) for purposes other than Business Use ("Non-Business Use"), but Services Users are required to keep Non-Business Use to a minimum and to comply with the requirements of this policy when engaging in Non-Business Use of Electronic Services. This policy discusses acceptable usage of Electronic Services for both Business Use and Non-Business Use.

As a Healthfully Service User, you understand and agree to the following:

- Electronic Services, including the equipment used to access or provide them, are company property of Healthfully, and no Service User or third party has any right to, or expectation of, privacy in their access or use.
- Healthfully reserves the right to intercept, reroute, monitor, retrieve, read and record any conversation, message or other electronic communication or related data sent, received or created by any Service User or third party.
- Healthfully may periodically monitor, audit and report on activities conducted by Service Users and third parties using the Electronic Services, including but not limited to all files, e-mail and voice mail, whether in transit or in storage.
- Service Users shall not access or use the data and databases that are part of the Electronic Services for any Non-Business Use under any circumstances.
- Services Users are responsible for keeping passwords and accounts secure, not sharing account information or access with any Service User (other than authorized Healthfully IT staff) or third party and changing passwords as required by authorized Healthfully IT staff.
- Postings by Service Users from a Healthfully account to newsgroups must be made only for Business Uses.
- Service Users shall (a) use extreme caution when opening suspicious e-mail attachments or when receiving communications over the Electronic Services from unknown parties, as these may lead to virus or identity theft events, and (b) report

any suspicious or unauthorized activity concerning the Electronic Services to authorized Healthfully IT staff as soon as possible.
- Service Users are reminded that electronic data (including messages, files, code, e-mail and voice mail) may still be retrievable by Healthfully even if deleted by the Service User.
- Service Users shall comply with all applicable laws, regulations, standards, and contracts in accessing or using the Electronic Services.

Guidelines

The following guidelines have been established to ensure that Services Users use the Electronic Services in an appropriate, ethical and professional manner. Service Users are prohibited from using Electronic Services for any unacceptable use, which includes (but is not limited to) the following activities:

- Accessing or disclosing any Healthfully or Healthfully client data, database, trade secret, proprietary information, company materials, or confidential information in violation of Healthfully's (or a Healthfully client's) confidentiality agreements or policies. This includes, but is not limited to, accessing any data or database concerning any client or client's employee (or their dependents) for use other than to perform the Healthfully engagement for which such data has been supplied or such database compiled.
- Creating, displaying, accessing, downloading, uploading, posting, forwarding, sending, distributing, storing, or viewing content which could have the effect of offending someone on the basis of his/her race, age, gender, sexual orientation, religious or political beliefs, national origin, disability or other protected characteristic.
- Creating, displaying, accessing, downloading, uploading, posting, forwarding, sending, distributing, storing, or viewing any sexually explicit materials or materials that may violate the Healthfully Sexual Harassment, EEO and/or other Workplace Violence policies, as they exist now or in the future.
- Exchanging, engaging in, supporting, or otherwise condoning any taunting, threatening, or otherwise hostile behavior.
- Conducting any business activities not related to Business Use.
- Soliciting for outside business ventures, charities, membership in any organization, political causes, or religious causes.
- Using chat rooms, instant messaging, or any similar technology for any Non-Business Use.
- Sending anonymous e-mail, using forged e-mail headers or another user's account to send e-mail, sending unsolicited commercial e-mail (also known as SPAM) or sending "chain" or "pyramid" e-mails.
- Downloading or installing any software, content or code without coordination and pre-approval by the IT Department. Such approval is required for purposes including (but not limited to) preventing license violations, unwanted content or viruses.
- Copying, installing, or downloading material that is protected by copyright, trademark, trade secret, patent, or other intellectual property rights in violation of any law, regulation or contract, or connecting to any service or installing any software that permits file sharing.

- Establishing direct or alternate Internet access by means other than those provided or approved by Healthfully as part of the Electronic Services, including (but not limited to) installation of any hardware or software that would enable users to obtain independent Internet access.
- Causing a slowdown, delay or congestion of the network supporting the Electronic Services, interfering with the work of others when accessing the network or Internet (including, but not limited to, accessing sites that provide streaming audio or video), introducing or distributing any malicious code or conducting any security exploit using the Electronic Services.
- Monitoring the use of Electronic Services by any other Service User or third party, port scanning or security scanning, circumventing user authentication or other security measures, (unless part of the Service User's job responsibilities with Healthfully).
- Conducting, supporting, engaging in or otherwise participating in unlawful activities.

Ownership and Handling of Information

All electronic data, code, files, conversations, messages or other communications or items of any kind accessed, exchanged, created or stored using any Electronic Services ("Information") are deemed "works made for hire" of Healthfully, and Healthfully shall own all right, title and interest, including patent rights, copyrights, trade secret rights, trademark rights and all other intellectual property rights in and relating to any and all such Information. Healthfully may (and may allow others to) use, reproduce, disseminate, alter and otherwise exploit any such Information (including, without limitation, any manner in which such activity may be recorded or remembered or modified) or derivatives or extensions or imitations in any manner. Service Users hereby assign to Healthfully all rights needed to confirm Healthfully's ownership rights in such Information. Service Users shall not have any right to make, obtain or remove copies of such Information during or after termination of their work or employment with Healthfully.

All Information shall be subject to deletion by Healthfully in order to preserve the integrity of the Electronic Services or to comply with the retention policies established by Healthfully from time to time.

Healthfully reserves the right to disclose any Information to law enforcement agencies without the prior consent of the Service User or any third party.

Healthfully's Right to Monitor; Consequences of Violations or Abuse

As noted above, all company-supplied technology, including computer systems and company-related work records, and Information belong to Healthfully. Healthfully routinely monitors usage patterns of the Electronic Services for communications by Service Users and third parties. Although Service Users may explore the vast resources available on the Internet for Business Uses, Service Users may access the Internet solely as permitted by this policy.

Since all aspects of the Electronic Services are Healthfully owned, access to and use of the Electronic Services is governed by this policy and all other Healthfully company policies at all times. Any employee who violates this or any other Healthfully policy or abuses the

privilege of Healthfully facilitated access to or use of the Electronic Services may be denied access to one or more parts of the Electronic Services at Healthfully's sole discretion, and if appropriate, be subject to disciplinary action up to and including termination. Violations of this policy should be reported to the Information Security Officer.

Questions Regarding the Use of the Electronic Services

If you have questions regarding the appropriate use of the Electronic Services, contact the Information Security Officer.

Appendix 1

Agreement to Comply with Information Security Policies and Procedures

Although Healthfully has specialists devoted to information security, it is the responsibility of users to comply with all information security policies and procedures. When the undersigned requests a userID on any Healthfully information system, he/she acknowledges that he/she is a "user" as defined in *Healthfully Information Security Policies and Procedures*. As a user, the undersigned additionally acknowledges that he/she must comply with the security measures dictated by both "owners" and "custodians," as defined in the information security manual.

As a user, the undersigned acknowledges that he/she is a fiduciary in possession of Healthfully information resources. This means that the undersigned must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

The undersigned has read and understood the policies and procedures described therein. The undersigned agrees to abide by the policies and procedures described therein as a condition of continued employment. The undersigned furthermore understands that violators of these policies and procedures are subject to disciplinary measures including privilege revocation and/or employment termination. The undersigned understands that access to Healthfully information systems is a privilege which may be changed or revoked at the sole discretion of Healthfully management, and which automatically terminates upon departure from Healthfully.

The undersigned certifies that he/she has received a copy of the *Healthfully Information Security Policies and Procedures* and Company's Acceptable Use Policy for Electronic Communications Services, Equipment and Data attached in Exhibit A herein for future reference.

The undersigned also agrees to promptly report all violations or suspected violations of information security policies and procedures to the VP of Development.

_____ _____

User's signature Date

_____

User's name in block capital letters