HIPAA Security
Policies and Procedures

Help at Home, LLC

(“Help at Home”)

HIPAA Security Officer – John Melby

Phone: (312) 755-3257
Fax: (312) 704-1126

Effective Date / Last Update: July 2020

TABLE OF CONTENTS

SP1 - Information Security Strategy

Purpose:

1. The purpose of this Information Security Program is to provide reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of information assets and electronic Protected Health Information ("EPHI") by protecting those assets from unauthorized access, modification, destruction, use or disclosure as required by the including, but not limited to, the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH") as expanded by the Affordable Care Act of 2010 ("ACA") and the HIPAA Omnibus Rule of 2013 ("HIPAA Omnibus Rule") and the Security Standards for the Protection of Electronic Protected Health Information, found at 45 CFR Part 160 and Part 164, Subparts A and C ("HIPAA Security Rule") (collectively, the "HIPAA Security Requirements").
2. Help At Home maintains an Information Security Program that complies with core business objectives as well as applicable state and federal regulations, including the HIPAA Security Requirements. This program as described by Help At Home's security and information technology ("IT") policies and the supporting plans and procedures will clearly state the objectives, responsibilities, and enforcement requirements of Help At Home.
3. The purpose of the Help At Home Information Security Program is to:
   a. Establish policies, procedures, plans, and standard tools to secure information in compliance with state and federal security requirements, using minimum levels of industry standards.
   b. Support Help At Home and Help At Home's mission to provide continuity of service to participant/ individuals.
   c. Maintain unbroken trust with participant/ individuals and stakeholders through practice of good stewardship of information assets.

Scope:

1. This policy applies to all types of sensitive information and EPHI, including such information that is created, received, or held by Help At Home. This information will be protected in any form including, but not limited to paper, electronic, or oral.
2. This policy applies to all Help At Home personnel including, but not limited to full-time employees, part-time employees, trainees, contractors, temporary workers, and anyone else granted access to Help At Home assets, resources, EPHI and/or sensitive data ("Help At Home Workforce").

Policy:

1. Help At Home will implement safeguards determined to be reasonable and appropriate to protect its information assets to maintain the confidentiality, integrity, and availability of those assets.
2. Security policies, plans, and procedures created in support of this Information Security Policy, are organized in five categories (sections) and address at a minimum:
   a. Administrative safeguards:
      i. Risk management
      ii. Sanction policy
      iii. Information system activity review
      iv. Assigned security responsibility

v. Termination procedures

vi. Information access management

vii. Security awareness and training

viii. Protection from malicious software

ix. Password management

x. Security incident procedures

xi. Response and reporting

xii. Data backup plan

xiii. Disaster recovery plan

xiv. Business associate agreement and other arrangements

b. Physical safeguards

i. Facility security plan

ii. Workstation use

iii. Workstation security

c. Technical safeguards

i. Access control

ii. Automatic logoff

iii. Encryption and decryption

iv. Integrity

v. Encryption

d. Data Breach

i. Data Breach Management

ii. Data Breach Notification

e. Other Policies

i. Information classification

ii. Network security

iii. Email security

iv. Remote access

v. Portable devices

vi. Wireless security

3. In addition, all security policies, and procedures shall be reviewed and evaluated (based on any environmental and operational changes) on an annual basis by the Help At Home Security Officer, as defined in the Assigned Security Responsibility Policy, and his/her designee(s).

Procedure(s): Procedures developed in support of the Information Security Policy will address (but are not limited to):

1. Information system activity review
2. Workforce clearance

3. Termination
4. Security incident handling
5. Access authorization, establishment, and modification
6. Contingency operations procedures
7. Physical access control and validation procedures
8. Updating maintenance records
9. Workstation use
10. Media disposal and re-use
11. Accountability
12. Data backup and storage procedures
13. Emergency access
14. Automatic logoff

Responsibilities:

1. All Help At Home Workforce are responsible for compliance with all security policies.
2. The Security Officer is responsible for:
   a. The development, implementation, and maintenance of Help At Home security policies
   b. Working with employees to develop procedures and plans in support of security policies

Retention: Every policy and procedure revision/replacement will be maintained for a minimum of six years from the date of its creation or when it was last in effect, whichever is later. Other Help At Home requirements may stipulate a longer retention.

Compliance: Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and standards such as HIPAA, HITECH and others.

Contact:

Help at Home, LLC.
33 S. State St., Suite 500
Chicago, IL 60603
ATTN: John Melby, Security Officer
jmelby@helpathome.com
Phone: (312) 755-3257
Fax: 312-704-0022

Policy History: Initial effective date: January 1, 2016

SP2 - Risk Management Policy

Purpose: The purpose is to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.

Policy: Help At Home will implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with impacted regulations.

Procedure(s):

1. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce the risk to an acceptable level.
2. Risk management related activities are essential to help identify critical resources needed to support Help At Home and the likely threat to all such resources.
3. The principal goal of Help At Home's risk management policy is to protect the organization, especially its sensitive information, and its ability to perform its mission.
4. The objective of performing risk management is to enable Help At Home to accomplish its mission by:
   a. Better securing systems that store, maintain, process or transmit sensitive information
   b. Enabling management to make well-informed risk management decisions to justify the expenditures that are a part of the IT and other budgets
   c. Assisting management in authorizing or evaluating systems on the basis of supporting documentation resulting from the performance of risk management
5. Risk management consists of three phases. The activities that Help At Home will conduct in each phase are as follows:
   a. Phase I: Risk Assessment
      i. System characterization
      ii. Threat identification
      iii. Vulnerability identification
      iv. Safeguard analysis
      v. Likelihood determination
      vi. Impact analysis
      vii. Risk Determination
      viii. Safeguard recommendations
      ix. Results documentation
   b. Phase II: Risk Mitigation
      i. Prioritize actions
      ii. Evaluate recommended safeguard options
      iii. Conduct cost-benefit analysis
      iv. Select safeguards
      v. Assign responsibility
      vi. Develop safeguard implementation plan
      vii. Implement selected safeguards

c. **Phase III: Evaluation and Assessment (Residual Risk)**

i. Evaluate safeguards deployed

ii. Evaluate security policies

Responsibilities:

1. The Security Officer has the responsibility to:

a. Ensure that appropriate risk analysis covering, at a minimum, all sensitive information are performed at a frequency of at least once a year

b. Approve risk mitigation plans, risk prioritization, and the elimination or minimization of risks

c. Facilitate timely actions, decisions and remediation activities

2. The Security Officer must be supported by all system owners, data owners and other managers to identify and prioritize risks to sensitive information. Risk management is an essential management function at Help At Home.

Policy History: Initial effective date: January 1, 2016

SP3 - Sanction Policy

Purpose: The purpose of this policy is to apply appropriate sanctions against Help At Home Workforce who fail to comply with the security policies or procedures of Help At Home.

Policy: Help At Home will ensure all Help At Home Workforce comply with the security policies of the organization as well as state and federal regulations such as HIPAA and the HITECH Act by applying sanction and disciplinary actions appropriate for the breach of policy.

Procedure(s):

1. Help At Home will appropriately discipline Help At Home Workforce for any violation of security policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings and immediate dismissal from employment.
2. Help At Home Workforce who knowingly and willfully violate state or federal law for improper use or disclosure of a participant's/ individual's information are subject to criminal investigation and prosecution or civil monetary penalties.
3. Help At Home will record all disciplinary actions taken in the employment records of the Help At Home Workforce.
4. Help At Home will investigate any security incidents or violations and mitigate to the extent possible any negative effects of the incident a timely manner.
5. Help At Home and Help At Home Workforce will not intimidate or retaliate against any workforce member or participant/ individual that reports the incident.
6. Help At Home will ensure all sanctions in this policy are consistent with Human Resources Policies.

Responsibilities:

1. All Help At Home Workforce are responsible for compliance with any sanction that is applied to them under this policy.
2. The Security Officer is responsible for reviewing reported security incidents and violations of security policy and levying, based on the gravity of the breach, appropriate sanctions upon the Help At Home Workforce.

Policy History: Initial effective date: January 1, 2016

SP4 - Information System Activity Review Policy

Purpose: The purpose is to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Policy: Help At Home will clearly identify all critical systems that process sensitive information. Help At Home will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.

Procedure(s):

1. Help At Home will clearly identify all critical systems that process sensitive information. Help At Home will implement security procedures to regularly review the records of information system activity on all such critical systems that process sensitive information.
2. The information that will be maintained in audit logs and access reports including security incident tracking reports must include as much as possible, of the following, as reasonable and appropriate:
    a. User IDs;
    b. Dates and times of log-on and log-off;
    c. Terminal identity, IP address and/or location, if possible; and
    d. Records of successful and rejected system access attempts.
3. Help At Home will attempt wherever reasonable, appropriate, and technically feasible to record:
    a. Who (Unique User ID);
    b. What action (Read, write, edit, delete, print, etc.);
    c. What data (Server, DB, instance, table, row, field);
    d. When (Enterprise wide timestamp);
    e. From; and
    f. Where (Terminal ID, IP address, local or remote access).
4. Safeguards must be deployed to protect against unauthorized changes and operational problems including:
    a. The logging facility being deactivated;
    b. Alterations to the message types that are recorded;
    c. Log files being edited or deleted; and
    d. Log file media becoming exhausted, and either failing to record events or overwriting itself.
5. Procedure related to Information System Activity Review:
    a. Security Incident Procedures

Responsibilities:

1. The Security Officer will clearly identify:
    a. The systems that must be reviewed;
    b. The information on these systems that must be reviewed;
    c. The types of access reports that are to be generated;

d. The security incident tracking reports that are to be generated to analyze security violations; and

e. The individual(s) responsible for reviewing all logs and reports.

2. When determining the responsibility for information review, a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Policy History: Initial effective date: January 1, 2016

SP5 - Assigned Security Responsibility Policy

Purpose: The purpose of this policy is to identify the Security Officer who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule 164.308(a)(2).

Policy: Help At Home will assign final responsibility of security to one individual who will be referred to as the Security Officer.

Procedure(s):

1. Help At Home will assign final responsibility of security to one individual who will be referred to as the Security Officer.
2. This individual's ultimate goal is to protect the confidentiality, integrity, and availability of critical information assets at Help At Home and to ensure compliance with applicable regulations.
3. Responsibilities of the Security Officer include (but are not limited to):
   a. Ensuring all policies, procedures, and plans required by regulations are developed, implemented, and maintained as necessary;
   b. Monitoring changes in legislation that may affect Help At Home and its security position;
   c. Monitoring changes and advances in technology that may affect Help At Home and its security position;
   d. Performing technical and non-technical evaluations or audits on security processes in order to find and correct weaknesses and guard against potential threats to security;
   e. Acting as an internal consultant and potentially as an external spokesperson for Help At Home in all issues related to security;
   f. Ensuring a system for reporting and responding to security incidents (as well as violations of regulations) is in place and functioning; and
   g. Delivering, on an ongoing basis, security awareness training to all members of the workforce.
4. If the Security Officer is not able to meet the requirements of this policy, or is no longer affiliated with the organization, Help At Home will assign these responsibilities to a new Security Officer. The appointment will not be left unfilled and will be documented with the Security Officer Declaration Log and organizational chart.

Responsibilities:

1. All Help At Home Workforce are responsible for supporting and providing assistance to the Security Officer whenever necessary when the Security Officer is acting in the role described under the policy section.
2. The Help At Home Security Officer, as defined by the Assigned Security Responsibility Policy, is responsible for all aforementioned responsibilities described in the policy section.
3. All management members are responsible for duly appointing a capable Security Officer and replacing that person if they are not able to fill their responsibilities or are no longer affiliated with the organization.

Policy History: Initial effective date: January 1, 2016

SP6 - Workforce Security Policy

Purpose: The purpose of this policy is to implement policies and procedures to ensure that all members of the workforce have appropriate access to sensitive information and to prevent those workforce members who should not have access from obtaining access to sensitive information.

Policy: Help At Home shall ensure that Help At Home Workforce as well as contractors and others are only accessing those systems and information to which they are authorized.

Procedure:

1. Help At Home Workforce as well as contractors and others shall access only those systems and information to which they are authorized.
2. Access will be provided on the basis of the Information Access Management Policy.
3. The termination of any member of the workforce will result in the immediate implementation of the activities identified in the Termination Procedures Policy.
4. All Help At Home Workforce will be appropriately trained so they understand Help At Home's policies related to accessing authorized information only.
5. Help At Home will continually assess potential risks and vulnerabilities to sensitive information in its possession and develop, implement, and maintain appropriate security measures so that access is only provided to authorized members of the workforce and all such information access is restricted to the minimum necessary to accomplish their job role or function.

Responsibilities: The Security Officer is responsible for determining the appropriate classification of information, such as sensitive information and maintains a list that details the type of access for each individual.

Policy History: Initial effective date: January 1, 2016

SP7 - Termination Procedure

Purpose: The purpose is to implement procedures for quickly, securely and completely terminating access to sensitive information when the employment of a workforce member or other arrangement ends.

Policy: Help At Home will terminate access to all systems and facilities when any Help At Home Workforce or entity Help At Home has other arrangements with has been terminated or no longer requires access to information or facilities in order to perform their assigned job role.

Procedure(s):

1. Any termination of Help At Home Workforce or other arrangement with must immediately result in the Human Resources (HR) and the Information Technology (IT) departments coordinating their activities to ensure:
   a. Password access is immediately revoked;
   b. Access to all systems and applications is revoked;
   c. Removal from any systems or applications that processed sensitive information;
   d. All digital certificates are revoked;
   e. Any computing equipment, resources, documentation, or other assets issued or provided are returned;
   f. Any tokens or smart cards issued are disabled and returned;
   g. Any keys and IDs provided during their employment are returned, and
   h. The workforce member is not provided any access to their desk or office or, if provided, the access is limited and carefully supervised.
2. If listed items cannot be returned to Help At Home for any reason, compensatory controls must be implemented such as changing locks or remotely disabling tokens. IT will provide feedback to HR on the success or failure of access termination.
3. Termination of access will be verified and segregation of duties will be applied to ensure immediate and complete termination of all access including electronic and physical.
4. Human Resources must conduct an exit interview and document any issues or concerns related to the workforce member or other arrangement with. (See HR Policies for further details).

Responsibilities: The Security Officer is responsible for ensuring that all activities identified in this Termination Procedure document occur.

Policy History: Initial effective date: January 1, 2016

SP8 - Information Access Management Policy

Purpose: The purpose is to implement policies and procedures for authorizing access to sensitive information.

Policy: Help At Home Workforce are granted access only to that sensitive information to which they are authorized in order to perform their job role or associated job function.

Procedure(s):

1. Help At Home Workforce are to be granted access only to that sensitive information to which they are authorized in order to perform their job role or associated job function.
2. Help At Home Workforce will be trained on appropriate access to sensitive information and on information access controls.
3. Safeguards, such as role-based access control, context-based access control, mandatory access control or discretionary access control, will be used as appropriate to control access to sensitive information.
4. Help At Home will develop security policies to identify core activities in the areas of:
    a. Isolating health care clearinghouse function
    b. Access authorization
    c. Access establishment and modification.

Responsibilities:

1. Help At Home Workforce are responsible for ensuring that they obtain only the type and amount of sensitive information necessary to carry out their assigned job role or function.
2. The Security Officer is responsible for:
    a. Determining and granting the appropriate access to sensitive information.
    b. Leading activities that bring Help At Home into compliance with legislative requirements.

Policy History: Initial effective date: January 1, 2016

SP9 - Security Awareness and Training Policy

Purpose: The purpose is to implement a security awareness and training program for all members of Help At Home Workforce, including management.

Policy: Help At Home will ensure that all Help At Home Workforce have been trained in, and fully understand the security policies and procedures of Help At Home. In addition, all Help At Home Workforce will be trained how to identify, report, and prevent potential security incidents.

Procedure(s):

1. Help At Home understands that people, not necessarily technology, are often the largest threat to the security of sensitive information in the organization.
2. Security training will be an ongoing activity at Help At Home. Periodic security reminders are part of the ongoing training activity. Help At Home will ensure that all Help At Home Workforce have been trained in and fully understand the security policies and procedures of Help At Home. In addition, all Help At Home Workforce will be trained how to identify, report, and prevent potential security incidents.
3. Help At Home will develop security policies to identify core activities in the areas of:
   a. Security reminders;
   b. Protection from malicious software;
   c. Log-in monitoring, and
   d. Password management.

Responsibilities:

1. All Help At Home Workforce are responsible for understanding and following all security-related policies and procedures.
2. The Security Officer is responsible for:
   a. Ensuring all Help At Home Workforce understand and follow security-related policies and procedures
   b. Maintaining an ongoing security awareness program at Help At Home
   c. Ensuring all Help At Home Workforce understand and use the installed anti-virus software
   d. Keeping all anti-virus software up-to- date on all systems storing, processing, or transmitting EPHI
   e. Leading activities that bring Help At Home into compliance with regulatory requirements.

Policy History: Initial effective date: January 1, 2016

SP10 - Protection from Malicious Software Policy

Purpose: The purpose is to implement procedures for guarding against, detecting, and reporting malicious software.

Policy: Help At Home will deploy malicious software identification, prevention, and removal technology at the perimeter of its network, on all servers (including email servers), and on individual end-user systems.

Procedure(s):

1. Help At Home will subscribe to updates to malicious software checking programs, which is McAfee.
2. Help At Home will ensure that updates are being received and applied on a daily basis at a minimum.
3. Help At Home conduct security training that will include information on:
    a. Potential harm that can be caused by malicious software
    b. Prevention of malicious software such as viruses
    c. Steps to take if a malicious software such as a virus is detected

Responsibilities:

1. All Help At Home Workforce of this policy are responsible for:
    a. Not configuring or introducing any modifications to systems or applications to prevent the execution of malicious software checking programs;
    b. Immediately contacting the Security Officer or respective manager by phone or walk-in – not by email – if there are any indications of a threat or malicious software infection; and
    c. Participating in all security awareness training programs and applying the knowledge in preventing, detecting, containing and eradicating malicious software.
2. The Security Officer is responsible for:
    a. Ensuring that malicious software checking programs are installed both on the perimeter of the network and on individual end-user systems;
    b. Identifying all critical systems and network components that are vulnerable to malicious software; and
    c. Implementing malicious software checking capability on all such identified systems.

Policy History: Initial effective date: January 1, 2016

SP11 - Password Management Policy

Purpose: The purpose is to implement procedures for creating, changing and safeguarding passwords.

Policy: Help At Home will implement procedures and training to ensure that all Help At Home Workforce, including privileged users and IT administrators, create secure, complex passwords, modify those passwords on a periodic and regular schedule, and safeguard their passwords appropriately.

Procedure(s):

1. Help At Home requires that:
   a. All passwords must be changed at least once every 180 days;
   b. All production system-level 'privileged account (i.e. Administrator, root, etc.) passwords must be part of the Security Officer's global password management database;
   c. User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user;
   d. Passwords must not be inserted into email messages or other forms of electronic communication; and
   e. Where the Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of "public," "private," and "system," and must be different from the passwords used to log in interactively. A keyed hash must be used where available (for example, SNMPv3).
2. Users must select strong passwords.
   a. Strong passwords have the following characteristics:
      i. Is at least eight characters long;
      ii. Does not contain your user name, real name, or company name;
      iii. Does not contain a complete word;
      iv. Contains a mixture of upper and lowercase letters, numbers, and symbols;
      v. Is significantly different from previous passwords; and
      vi. Not contain 4 consecutive characters used from the previous password.
   b. Poor, weak passwords have the following characteristics:
      i. Less than eight characters;
      ii. A word found in a dictionary (English or foreign);
      iii. A common usage word such as:
         A. Names of family, pets, friends, co-workers, fantasy characters, etc.;
         B. Computer terms and names, commands, sites, companies, hardware, software;
         C. Birthdays and other personal information such as addresses and phone numbers; or
         D. Word or number patterns (e.g., aaabbb, qwerty, zyxwvuts, 123321, etc.).
      iv. Any of the above spelled backwards; and
      v. Any of the above preceded or followed by a digit (for example, secret1, 1secret).

3. Systems that authenticate must require passwords of users and must block access to accounts if more than six unsuccessful attempts are made.

4. The following password guidelines must be followed:

   a. Don’t reveal a password over the phone to ANYONE;

   b. Don’t reveal a password in an unsecured email message;

   c. Don’t talk about a password in front of others;

   d. Don’t hint at the format of a password, like, “my family name”;

   e. Don’t reveal a password on questionnaires or security forms;

   f. Don’t share a password with family members; and

   g. Don’t reveal a password to co-workers.

5. If someone demands a password, refer them to this document or have them call someone in the Information Security Department or contact the Security Officer.

6. The “Remember Password” feature of applications such as Internet Explorer, Google Chrome or operating systems such as Windows must not be used.

7. Passwords must not be written down and stored anywhere in a Help At Home Workforce office.

8. Passwords must not be stored on ANY computer system (including smartphones or similar devices) without suitable encryption.

Responsibilities:

1. All Help At Home Workforce are responsible for:

   a. Not sharing their passwords with anyone, including administrative assistants or secretaries; and

   b. Treating all passwords as sensitive, confidential information.

2. The Security Officer is responsible for:

   a. Ensuring the implementation of the Password Management Policy; and

   b. Authorized the periodic and/or random password cracking or guessing and requiring any identified passwords to be changed by the user.

Policy History: Initial effective date: January 1, 2016

SP12 - Security Incident Procedures

Purpose: The purpose is to thoroughly address security incidents.

Policy: Help At Home will create processes for the identification, reporting, and timely response to real or potential violations of information security or a material breach of any part of Help At Home's security policies.

Procedure(s):

1. Help At Home will maintain procedures for identifying security incidents. A security incident is any breach of security policy, or any activity that could potentially put sensitive information at risk of unauthorized use, disclosure, or modification.
2. A breach, as defined under the HITECH Act, may have occurred if the incident involved EPHI. A breach is defined as the unauthorized acquisition, access, use, or disclosure of protected information as defined below, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. If a breach has occurred, Help At Home Workforce must immediately follow the instructions in the Data Breach Management Policy.
3. Incidents will be classified as "serious" or "non-serious." Non-serious incidents generally have the following characteristics:
   a. It is determined that there was no malicious intent (or the attack was not directed specifically at Help At Home); and
   b. It is determined that no sensitive information was used, disclosed, or damaged in an unauthorized manner.
4. Serious incidents generally have the following characteristics:
   a. It is determined that there was malicious intent and/or an attack directed specifically at Help At Home
   b. It is determined that sensitive information, including EPHI, may have been used, disclosed, or damaged in an unauthorized manner or that this incident may construe a data breach.
5. All Help At Home Workforce will report any security incident to the Security Officer that they become aware of or suspect, as soon as practical.
6. Workforce members will not disclose the incident information to anyone other than the Security Officer, Privacy Officer, or Help At Home management member, and will not disclose any information about the incident to anyone or in any place outside of Help At Home.
7. Help At Home will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature.
8. Incidents characterized as serious by the Security Officer will be responded to immediately and reported to all upper-level management.
9. Help At Home will attempt to mitigate any harmful effects, when possible, of security incidents that affect participant/ individual information.
10. In addition to this Security Incident Procedures policy, refer to Response and Reporting, for procedures related to security incident response.

Responsibilities:

1. All Help At Home Workforce are responsible for:

a. Staying aware of and identifying potential security incidents;

b. Reporting any suspected security incident to the Security Officer; and

c. Assisting the Security Officer in ending the security breach and mitigating its harmful effects, if possible.

2. The Security Officer is responsible for:

a. Maintaining all security incident-related policies and procedures;

b. Characterizing all reported security incidents as “serious” or “non-serious” as per the guidelines outlined above. The Security Officer may take into account their professional expertise and experiences when making these characterizations;

c. Maintaining procedures for responding to security incidents;

d. Documenting all reported security incidents and their outcomes; and

e. Leading activities that bring Help At Home into compliance with regulatory requirements.

3. The Security Officer and other members of management are jointly responsible for:

a. Mitigating, to the extent possible, any harmful effects of security incidents; and

b. Deciding when it is appropriate to contact law enforcement officials about a security incident that has been characterized as serious.

Policy History: Initial effective date: January 1, 2016

SP13 - Response and Reporting Policy

Purpose: The purpose is to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to Help At Home, and document security incidents and their outcomes.

Policy: Help At Home will:

1. Identify, research, and respond to any suspected security incidents;
2. Mitigate, to the extent practicable, any harmful effects of any suspected or actual security incidents; and
3. Maintain appropriate documentation for all security incidents.

Procedure(s):

1. If the security incident constitutes a breach of EPHI, please immediately follow the instructions in the Data Breach Management Policy.
2. This policy requires addressing the following seven steps:
    a. Prepare for a Security Incident
    b. Detect and Report Security Incidents
    c. Assemble the Incident Response Team
    d. Limit Further Damage
    e. Gather Evidence
    f. Fix the Damage
    g. Analyze the Incident
3. **Step 1: Prepare for a Security Incident**
    a. Every network may at some point be a victim of a computer security incident. System and network administrators must be prepared for security incidents and be able to respond quickly to minimize and repair the damage. Some critical steps that must be addressed are:
        i. Identify the Security Incident Response Team;
        ii. Acquire specialized security training;
        iii. Verify the deployment of Intrusion Detection Systems (IDS); and
        iv. Verify Data Backup Plan and its implementation.
    b. The key is to be prepared so that in the event of a security incident the response is swift and comprehensive in resolving the damage.
4. **Step 2: Detect and Report Security Incidents**
    a. As soon as a security incident is detected it should be immediately reported to the Security Incident Response Team or the Security Officer.
    b. A formal reporting procedure should be established, together with an incident response procedure, setting out the action to be taken on receipt of an incident report.
    c. All Help At Home Workforce should be made aware of the procedure for reporting security incidents, and should be required to report such incidents as quickly as possible.
    d. Suitable feedback processes should be implemented to ensure that those reporting incidents are notified of results after the incident has been dealt with and closed.

e. These incidents should be used in user awareness training as examples of what could happen, how to respond to such incidents, and how to avoid them in the future.

f. All users of information services should be trained to note and report any observed or suspected security weaknesses in, or threats to, systems or services. They should report these matters either to their management or to the Security Officer as quickly as possible. Users should be informed that they should not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, as testing weaknesses might be interpreted as a potential misuse of the system.

g. Procedures will also be established for reporting malfunctions such as those related to software, hardware or any other type.

5. Step 3: Assemble the Incident Response Team

a. The Security Incident Response Team must meet to evaluate and determine the potential cause of the incident. The following actions should be considered by the team:

i. Evaluate and document symptoms of the problem and any messages appearing on the screen;

ii. Isolate the affected computer, if possible, and stopping the use of it;

iii. Immediately alert the appropriate contact; and

iv. Immediately report the matter to the information security manager.

b. Users should not attempt to remove the suspected software unless authorized to do so.

c. Appropriately trained and experienced staff authorized by the Security Incident Response Team should carry out recovery activities.

6. Step 4: Limit Further Damage

a. Once the initial data has been collected, immediate steps need to be taken to minimize the spread of the damage. These steps may include:

i. Disable Internet access;

ii. Disable file servers, email servers, communication devices and other systems;

iii. Isolate impacted workstation(s), if possible, and stopping their use; and

iv. If equipment is to be examined, disconnect it from any organizational networks before being examined. Portable media should not be transferred to other workstations and systems should not be powered off unless absolutely necessary.

7. Step 5: Gather Evidence

a. The Security Incident Response Team must gather all possible evidence to fully understand the type of attack and its scope. The team needs to address questions such as:

i. How many systems are impacted?

ii. What levels of privileges were accessed?

iii. How widespread is the vulnerability?

iv. How far into the internal systems did the intruder get?

v. Which systems have been compromised?

vi. Any risk to sensitive information stored by systems?

b. All of the information collected should be thoroughly documented and reported. Dedicated systems should be used for incident analysis and forensics. The involved Workforce member should be trained in the use of such applications.

8. Step 6: Fix the Damage

a. Having gathered all the evidence, the Security Incident Response Team must lead eradication efforts.

b. Malicious files should be deleted, removed or replaced.

c. User accounts and associated passwords may need to be modified or re-created – if there was any evidence of unauthorized access.

d. Data may need to be restored from trusted backups.

e. After the impacted systems are cleaned and protected, they may be brought back online.

f. The team must monitor these systems and their infrastructure for other similar, subsequent incidents.

9. Step 7: Analyze the Incident

a. The Security Incident Response Team re-groups to do a post-event de-briefing.

b. The objective of the de-briefing is to assess the incident, the response, and identify any specific areas of concern. The team must have a full and complete understanding of the incident and how to prevent such incidents from occurring in the future.

c. The team should conduct a review of mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored. This information should be used to identify recurring or high impact incidents or malfunctions. This may indicate the need for enhanced or additional controls to limit the frequency, damage and cost of future occurrences, or to be taken into account in the security policy review process.

d. Finally, there should be a formal disciplinary process for employees who have violated organizational security policies and procedures. Such a process can act as a deterrent to employees who might otherwise be inclined to disregard security procedures.

Responsibilities:

1. All Help At Home Workforce are responsible for:

a. Immediately reporting any and all suspected violations of information security to the Security Officer. All incident reporting and response activities must be conducted strictly on a need-to-know basis.

2. The Security Officer is responsible for:

a. Training all members of the workforce on appropriate reporting of security violations.

b. Determining the appropriate level of response to a security incident. All such responses must be in accordance with established policies and procedures.

c. At a minimum, the Security Officer and/or his/her team must immediately consider a response that includes:

i. Disconnecting the affected system from the network (should not remove power from the system);

ii. Determining if the incident is accidental or intentional;

iii. Identifying all system-related information such as:

A. Hardware address;

B. System name;

C. IP address;

D. Sensitive data processed by the system;

E. Applications installed on the system; and

F. Location of the system; and

d. Completing a Security Incident Report for each security incident with as much information as possible about the following:

i. Contact information of the person reporting the incident (name, phone, address, email);

ii. Date and time of the incident;

iii. Detailed description of the incident; and

iv. Any further information, such as unusual activities or individuals associated with the incident.

Policy History: Initial effective date: January 1, 2016

SP14 - Data Backup Plan

Purpose: The purpose is to establish and implement procedures to create and maintain retrievable exact copies of sensitive information in the event of equipment failure or damage.

Policy:

1. Help At Home will create and maintain exact, retrievable copies of sensitive information.
2. Help At Home will ensure that sensitive data is backed up to disk, tape, or a combination of those technologies on a regular basis so as to minimize the loss of data in the event of an incident or disaster.
3. Help At Home will ensure that backup media is periodically tested to ensure suitable quality and reliable data restoration.

Procedure(s):

1. In developing the backup schedule, the Security Officer will consider factors such as:
   a. What data (systems, files, directories, and folders) should be backed up?
   b. How frequent are backups done?
   c. Who is responsible/ authorized to retrieve the media?
2. A backup schedule should include incremental backups each weekday, at different times of the day; full backups on weekends, and replication to the alternative operating facility.

Responsibilities:

1. The Security Officer will be responsible for implementing the requirements of the data backup plan.

Policy History: Initial effective date: January 1, 2016

SP15 - Disaster Recovery Plan

Purpose:

1. The purpose is to establish and implement as needed procedures to restore any loss of data.
2. The Disaster Recovery Plan ("DRP") applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. A disaster recovery plan refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency.
3. A disaster recovery plan provides a blueprint to continue business operations in the event that a catastrophe occurs. The disaster recovery plan must include contingencies for the period of time of the disaster and until the recovery plan can be completely implemented. The price for not developing a disaster recovery plan is that Help At Home may find it difficult to continue to be in business or potentially suffer a significant loss.

Policy: Help At Home will develop and maintain a Disaster Recovery Plan. The Security Officer will ensure the development of a Disaster Recovery Plan document.

Procedure(s): The Security Officer is to ensure the development of a Disaster Recovery Plan document. This document typically includes the following sections:

1. **Purpose:** a statement describing the goal of the disaster recovery plan.
2. **Scope:** identifies the specific locations/sites and critical systems that are a part of the disaster recovery plan.
3. **Assumptions:** identifies the foundation that the plan is based on.
4. **Team**: identifies the Team lead for the activity as well as members of the IT organization and others that will be involved in the disaster recovery process.
5. **Notification:** establishes the formal communication required to contact members to alert them of the incident.
6. **Damage Assessment and Reporting:** describes the process of analyzing the extent of damage to systems and sites and includes reports that identify recommendations for management.
7. **Activation:** describes the process to start disaster recovery activities.
8. **Recovery Operations:** describes the steps to recover critical systems and applications at the recovery site. This section would include information on data recovery based on the backed up data. See Data Backup Plan.
9. **Return to Normal Operations:** describes the procedures for the full recovery of all data and a complete return to normal processing of all business functions.

Policy History: Initial effective date: January 1, 2016

SP16 - Business Associate Agreements and Other Arrangements Policy

Purpose: The purpose is to obtain satisfactory assurances that Business Associates will appropriately safeguard all sensitive information in accordance with applicable regulations.

Procedure(s):

1. Each Business Associate that provides data transmission of protected health information to Help At Home(or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with Help At Home to allow Help At Home to offer a personal health record to participant/ individuals as part of its electronic health record, is required to enter into a Business Associate Agreement (BAA) with Help At Home.
2. Help At Home will establish the flow of sensitive information to all outside entities and identify how such information is transmitted, and the requirements for processing sensitive information at the business associate site.
3. Help At Home will review all existing BAAs and ensure that all such agreements are modified with Addendums or revised for compliance with impacted regulations.
4. The termination of an agreement with the Business Associate must result in return or destruction of all sensitive information by the business associate.
5. The Business Associate must train all members of their workforce that process or come into contact with sensitive information. This training must include awareness of the requirements of the appropriate regulation as well as information about the Business Associate's security policies and procedures.
6. Help At Home must reserve the right to take "reasonable steps" including canceling the BAA without penalty.
7. Help At Home may account for their own disclosures of participant/ individual information and then provide the name and contact info of the subcontractor for additional disclosure details. If requested by the participant/ individual, the Business Associate must account for their disclosures under a separate cover.

Responsibilities:

1. The Security Officer will:
   a. Review all Business Associate Agreements (BAAs) and modify them as necessary to ensure compliance with this standard; and
   b. Review the flow of sensitive information to identify all possible organizations that access sensitive information and may be required to execute a BAA or other legal agreement to ensure compliance with the applicable regulations.

Policy History: Initial effective date: January 1, 2016

SP17 - Facility Security Plan

Purpose: The purpose is to implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

Policy:

1. Help At Home will develop a Facility Security Plan to safeguard facilities and premises from unauthorized physical access, tampering or theft including the equipment present in all such facilities.
2. All equipment that collects, stores, maintains, processes, or transmits EPHI will be protected from unauthorized access at all times.

Procedure(s):

1. **Facility Security Plan**
   a. The Facility Security Plan must define the security perimeter of all buildings and sites.
   b. The Plan should ensure that all external doors are adequately secured against unauthorized access by installing locks, alarms, or other access control devices.
   c. The Facility Security Plan will be reviewed, and if necessary, updated at least once every quarter.
2. **Building Security**
   a. Internally, within buildings and facilities, all doors and windows must be locked by default.
   b. Intrusion detection capabilities must be evaluated to secure privileged internal areas.
   c. Physical barriers must be in place from the floor to the ceiling.
   d. Controls need to be deployed to protect against theft as well guard against fire, water or other damage. To the extent possible power and communications cabling must be located underground.
3. **Report Damages to Public Safety**
   a. Immediately report any break-ins, thefts, or tampering—suspected or actual—to Help At Home’s designated contact
   b. Report to law enforcement, if necessary.
   c. Document findings.
   d. Help At Home’s designated contact investigates the matter.
   e. After the investigation is completed, Help At Home makes its own report of the investigation and findings and provides that report to Administration with a copy to Information Systems.
   f. Recommendations are discussed and made for improvements with follow-up required.
4. **Access to Information Technology Offices and Data Centers**
   a. Only authorized individuals have access to the Information Technology offices and data centers.
   b. Information Technology staff is responsible for securing access to all network equipment and offices.
   c. Doors to the Information Technology offices are locked at all times, even when Information Systems staff members are present.

d. If you need to see an Information Technology staff member, call or page that staff member in advance of your visit.

Responsibilities:

1. The Security Officer will be responsible for ensuring the implementation of the requirements of the Facility Security Plan. The Security Officer is responsible for reviewing and updating the plan as necessary.

Policy History: Initial effective date: January 1, 2016

SP18 - Workstation Use Policy

Purpose: The purpose is to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access sensitive information.

Policy:

1. Help At Home will ensure that workstations and other computing devices with access to sensitive information are being used for work related purposes only.
2. All Help At Home workstations will be utilized in a secure, approved manner, by authorized Workforce member only, and in such a way that the confidentiality, integrity, and availability of EPHI are not jeopardized.
3. Help At Home will ensure that access is not permitted to Help At Home workstations by individuals that are not authorized Help At Home Workforce.

Procedure(s):

1. Workstations and other computing devices that are owned or operated by Help At Home with access to sensitive information are to be used for work-related purposes only. This includes, but is not limited to, Internet and Web access as well as the use of email at Help At Home.
2. Workforce members should not expect any level of personal privacy as their activities, emails, files, and logs may be viewed at any time by the Security Officer or other members of management in support of this and other policies and procedures.
3. Help At Home may revoke the access rights of any individual at any time in order to protect or secure the confidentiality, integrity, and availability of sensitive information or to preserve the functionality of electronic information systems.
4. Help At Home will implement reasonable and appropriate measures to secure its computing devices could be used to access sensitive information. These measures will include, but are not limited to the following:
    a. All user and administrator accounts must be protected by some form of authentication;
    b. All users accessing Help At Home's computing devices must have and use a unique user ID;
    c. Procedures must be maintained that implement security updates and software patches in a timely manner;
    d. Procedures must be maintained that require users to run an up-to-date anti-virus program on all computing devices at Help At Home;
    e. All unnecessary and unused services (or ports) must be disabled;
    f. Measures must be taken to physically protect computers that are located in public areas and portable computers, such as laptops and smartphones that could be removed from the premises; and
    g. Computers located in public areas will be situated as to block unauthorized viewing and/or will have screen savers that black out the screen. These computers will also have screen savers that automatically activate following a brief period of inactivity.

Responsibilities:

1. The Security Officer will be responsible for ensuring the implementation of this policy.

Policy History: Initial effective date: January 1, 2016

SP19 - Workstation Security Policy

Purpose: The purpose is to implement physical safeguards for all workstations that access sensitive information and to restrict access to authorized users.

Policy: Help At Home will implement physical safeguards for all workstations that access sensitive information to restrict access to authorized users only.

Procedure(s):

1. All members of the workforce will be trained on the appropriate and authorized use of workstations as part of the security awareness training.
2. Workstations must:
   a. Be positioned such that the monitor screens and keyboards are not within view of unauthorized individuals;
   b. Ensure the confidentiality of sensitive information;
   c. Employ a password-protected screen saver and/or workstation locking mechanism when the workstation is unattended.
3. Users of workstations must:
   a. Properly log off or shut down their workstation at the end of the business day;
   b. Prior to leaving the workstation during the day, users must log off; and
   c. Not store or post password information on the workstation or accessible anywhere in its vicinity.

Responsibilities:

1. All Help At Home Workforce are responsible for:
   a. Using Help At Home computing devices only for work-related purposes only; and
   b. Following all procedures implemented by the Security Officer related to this policy.
2. The Help At Home Security Officer is responsible for:
   a. Maintaining procedures required to support this policy; and
   b. Supporting and ensuring compliance by workforce members

Policy History: Initial effective date: January 1, 2016

SP20 - Access Control Policy

Purpose: The purpose is to implement technical policies and procedures for electronic information systems that maintain sensitive information to allow access only to those persons or software programs that have been granted access rights as specified by regulation or business process.

Policy: Help At Home will control access to its information assets and systems. Only individuals that have been formally authorized to view or change sensitive information will be granted access to that information.

Procedure(s):

1. Help At Home will control access to its information assets and systems. Only individuals that have been formally authorized to view or change sensitive information will be granted access to that information.
2. Access will be based upon Help At Home's Access Management Policy.
3. Each individual that accesses sensitive information via computer at Help At Home will be granted some form of unique user identification, such as a login ID. At no time will any workforce member allow anyone else to use their unique ID. Likewise, at no time will any workforce member use anyone else's ID.
4. Help At Home will establish an Emergency Access Procedure for gaining access to sensitive information during an emergency. Extraordinary care in safeguarding and documenting the use of the information will be exercised during this procedure.
5. Wherever reasonable and appropriate, Help At Home will establish role-based categories that identify types of information necessary for employees to do their jobs. Access to sensitive information will be granted based on these roles or functions that the individual performs within the organization.
6. Help At Home will maintain procedures for automatic logoff of systems that contain sensitive information after a period of inactivity. See Automatic Logoff Policy. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the computer is located.
7. Help At Home will evaluate and implement encryption and decryption solutions as an additional form of access control, where deemed reasonable and appropriate. These solutions will be implemented according to Help At Home's Encryption and Decryption Policy, and Encryption Policy, and when they are found to be:
    a. Technically sound and useable
    b. Financially reasonable
8. Help At Home will evaluate and implement additional procedural and technical control solutions as additional forms of access control, where deemed reasonable and appropriate according to Help At Home's policies.

Responsibilities:

1. All Help At Home Workforce are responsible for:
    a. Ensuring no other individual uses their unique ID;
    b. Never using another individual's unique ID; and
    c. Abiding by the terms of this policy
2. The Security Officer is responsible for:

a. Ensuring workforce members have access to only the sensitive information they need to do their jobs;

b. Creating and maintaining role-based access control based on the roles and functions workforce members perform in the organization;

c. Ensuring each workforce member has a unique user ID for access systems that contain sensitive information;

d. Maintaining Emergency Access Procedures;

e. Maintaining Automatic Logoff Procedures; and

f. Evaluating and implementing (when reasonable and appropriate) encryption and decryption solutions as a form of access control.

Policy History: Initial effective date: January 1, 2016

SP21 - Automatic Logoff Policy

Purpose: The purpose is to implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Policy:

1. Help At Home will maintain procedures for Automatic Logoff of systems that contain sensitive information after a period of inactivity.
2. Help At Home will configure all systems that support automatic logoff to require logoff after a predetermined period of time. If systems do not support automatic logoff capabilities, Help At Home will request those capabilities from the appropriate vendor and document all vendor responses.

Procedure(s):

1. Help At Home will maintain procedures for Automatic Logoff of systems that contain sensitive information after a period of inactivity.
2. The length of time that a user is allowed to stay logged on while idle will depend on the sensitivity of the information that can be accessed from that computer and the relative security of the environment that the system is located.
3. Help At Home will periodically inspect systems to ensure that the automatic session logoff capability is configured correctly.
4. If systems do not support automatic logoff capabilities, Help At Home will request those capabilities from the appropriate vendor and document all vendor responses in writing.

Responsibilities:

1. The Security Officer will be responsible for ensuring the implementation of the Automatic Logoff Policy.

Policy History: Initial effective date: January 1, 2016

SP22 - Encryption and Decryption Policy

Purpose:

1. The purpose is to implement a mechanism to encrypt and decrypt sensitive information including EPHI.
2. This policy, along with the Encryption Policy (policy 25), is intended to assist employees of Help At Home in making a decision about the use of encryption technologies as a method of protecting data stored on systems that process sensitive information.

Policy: Media which cannot be protected by other methods of access control shall utilize encryption and decryption to protect EPHI from unauthorized disclosure. Encryption and Decryption may also be utilized in combination with other access controls where indicated by risk analysis.

Procedure(s):

1. Help At Home will identify systems that require EPHI to be encrypted.
2. Help At Home will identify Help At Home Workforce who require encryption capabilities.
3. Help At Home will need to balance the challenge of protecting "data at rest" such as that defined in the Access Control standard of the HIPAA Security Rule against the increase in security technology complexity and administrative overhead including performance considerations and usability.
4. Help At Home will seriously review the viability of securing EPHI on critical databases, file servers, and on mobile devices such as laptops, smartphones, and portable flash drives.
5. Proven, standard algorithms such as AES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption.
6. Symmetric cryptosystem key lengths must be at least 128 bits.
7. Asymmetric crypto-system keys must be of a length that yields equivalent strength.
8. Help At Home key length requirements will be reviewed annually and upgraded as technology allows. All keys generated will be securely escrowed.
9. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Security Officer.
10. Help At Home will test encryption and decryption capabilities of products and systems to ensure proper functionality.

Responsibilities:

1. The Security Officer will be responsible for ensuring the implementation of the Encryption and Decryption Policy.

Policy History: Initial effective date: January 1, 2016

SP23 - Audit Controls Policy

Purpose: The purpose is to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use sensitive information.

Policy:

1. Help At Home will identify critical systems that require event auditing capabilities.
2. Help At Home will define the events to be audited on all such systems.
3. Help At Home will protect all collected logs from alteration or destruction.

Procedure(s):

1. Help At Home will identify critical systems that require event auditing capabilities.
2. Help At Home will define the events to be audited on all such systems. At a minimum, event auditing capabilities will be enabled on all systems that process, transmit, store, and/or maintain sensitive information. Events to be audited may include, and are not limited to, logins, logouts, and file accesses, deletions and modifications.
3. Audits may be conducted to:
   a. Ensure confidentiality, integrity, and availability of sensitive information.
   b. Investigate possible security incidents and ensure conformance to Help At Home security policies.
   c. Monitor user or system activity where appropriate.
4. Help At Home will ensure the protection of all audit reports and log files.
5. Help At Home will review the usage of software and application tools to review audit files.
6. When requested, and for the purpose of performing an audit, any access needed will be provided to authorized members of Help At Home security team. This access may include:
   a. User level and/or system level access to any computing or communications device.
   b. Access to information (electronic, hardcopy, and so on) that may be produced, transmitted, maintained, or stored on Help At Home equipment or premises.
   c. Access to work areas (labs, offices, cubicles, storage areas, and so on).
   d. Access to interactively monitor and log traffic on Help At Home networks.
7. Help At Home will protect all collected logs from improper alteration or destruction even by Help At Home privileged users such as Administrators or ROOT accounts.
8. Help At Home logs should seek to follow “Write Once, Read Many” standards so that they cannot be altered once they are written.

Responsibilities:

1. The Security Officer will be responsible for ensuring the implementation of the Audit Controls policy.

Policy History: Initial effective date: January 1, 2016

SP24 - Integrity Policy

Purpose: The purpose is to implement policies and procedures to protect sensitive information from improper alteration or destruction.

Policy:

1. Help At Home will review the results of risk analysis to identify the data that must be protected from improper alteration or destruction.
2. Help At Home will ensure that data is only altered by properly authorized members of the workforce or automated processes.

Procedure(s):

1. Help At Home will review the results of risk analysis to identify the data that must be protected from improper alteration or destruction. The files and associated directories where such data is stored will be checked for data integrity.
2. Help At Home will ensure that all sensitive information systems are designed to maintain data integrity.
3. Help At Home will train members of the workforce to report unauthorized data modification or destruction.
4. Help At Home will ensure that systems maintain the integrity of data altered by members of the workforce even if those members change their legal names, depart the organization, or are deceased after alterations have been made.

Responsibilities:

1. The Security Officer will be responsible for ensuring the implementation of the requirements of the Integrity policy.

Policy History: Initial effective date: January 1, 2016

SP25 - Transmission Encryption Policy

Purpose:

1. The purpose is to implement a mechanism to encrypt sensitive information including EPHI in transit whenever deemed appropriate.

2. The Encryption Policy is intended to assist employees of Help At Home when making decision about purchasing or developing software and other systems that make use of encryption technologies as a method of protecting "data in motion."

Policy:

1. Help At Home will evaluate the need for and use of encryption to maintain the confidentiality and integrity of sensitive information being transmitted over a network.

Procedure(s):

1. EPHI Transmissions to Help At Home Entities

a. To appropriately guard against unauthorized access to or modification of EPHI that is being transmitted from Help At Home Network's to a network outside of such networks, the procedures outlined must be implemented:

i. All transmissions of EPHI from the Help At Home networks to a network outside of the aforementioned networks must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said EPHI must be encrypted before transmission;

ii. Prior to transmitting EPHI from the Help At Home networks to a network outside of the aforementioned networks the receiving person or entity must be authenticated;

iii. All transmissions of EPHI from the Help At Home networks to a network outside of the aforementioned networks should include only the minimum amount of PHI. (See HIPAA Privacy Policies: Minimum Necessary and Safeguarding PHI.); and

iv. For transmission of EPHI from the Help At Home networks to a network outside of the aforementioned networks utilizing an email or messaging system, see "EPHI Transmissions Using Email or Messaging Systems" below.

2. EPHI Transmissions Using Electronic Removable Media

a. When transmitting EPHI via removable media, including but not limited to, floppy disks, CDROM, memory cards, magnetic tape and removable hard drives, the sending party must:

i. Use an encryption mechanism to protect against unauthorized access or modification;

ii. Authenticate the person or entity requesting said EPHI in accordance with HIPAA Security, Person or Entity Authentication procedures; and

iii. Send the minimum amount of said EPHI required by the receiving person or entity.

b. If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

3. EPHI Transmissions Using Email or Messaging Systems

a. The transmission of EPHI from Help At Home networks to the subject or person of the EPHI via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

i. The individual has been made fully aware of the risks associated with transmitting EPHI via email or messaging systems;

ii. The individual has provided written authorization to Help At Home to utilize an email or messaging system to transmit EPHI to them;

iii. The individual's identity has been authenticated; and

iv. The email or message contains no excessive history or attachments.

b. The transmission of EPHI from Help At Home to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

i. The receiving entity has been authenticated;

ii. The receiving entity is aware of the transmission and is ready to receive said transmission;

iii. The sender and receiver are able to implement a compatible encryption mechanism;

iv. No EPHI is contained in the non-encrypted areas of the communication; and

v. All attachments containing EPHI are encrypted.

c. Email accounts that are used to send or receive EPHI must not be forwarded.

4. 4. **EPHI Transmissions Using Wireless LANs and Devices**

a. The transmission of EPHI over a wireless network within the Help At Home networks is permitted if the following conditions are met:

i. The local wireless network is utilizing an authentication mechanism to ensure that wireless devices connecting to the wireless network are authorized; and

ii. The local wireless network is utilizing an encryption mechanism for all transmissions over the aforementioned wireless network.

b. If transmitting EPHI over a wireless network that is not utilizing an authentication and encryption mechanism, the EPHI must be encrypted before transmission.

c. The authentication and encryption security mechanisms implemented on wireless networks within the Help At Home networks are only effective within those networks. When transmitting outside of those wireless networks, additional and appropriate security measures must be implemented in accordance with this Policy.

5. 5. **Additional Requirements for Electronic Transmissions**

a. All encryptions mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

b. When transmitting EPHI electronically, regardless of the transmission system being used, Help At Home users must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the EPHI requested.

c. If the EPHI is being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of PHI should be transmitted.

Responsibilities:

1. All Help At Home Workforce are responsible for:
    a. Understanding and following all security related policies and procedures related to encryption
2. The Security Officer is responsible for:
    a. Ensuring all Help At Home Workforce understand and follow security related policies and procedures related to encryption

Policy History: Initial effective date: January 1, 2016

SP26 - Information Classification Policy

Purpose: The purpose is to address information classification categories, acceptable access and use of information such as EPHI and other sensitive information.

Policy: Help At Home will classify information as appropriate and according to its level of sensitivity.

Procedure(s):

1. All Help At Home information will be organized into two main classes. These classes are “Public” and “Confidential.”
2. Public information is information that can be shared freely with anyone inside or outside of the organization without the possibility of negative consequences. Public information includes, but is not necessarily limited to:
   a. General information about Help At Home such as the mission statement; and
   b. Most marketing information.
3. Confidential information includes all other information, such as sensitive information, (information that, when shared or disclosed, could possibly have a negative consequence). It is understood that there are varying levels of sensitive information, and the lengths employees should go to protect the information depends on the sensitivity.
4. Help At Home will rely on the professional judgment of the individual on a daily basis when using and disclosing confidential information. If an individual is unsure of the relative sensitivity of a piece of information, they could contact their supervisor or the Security Officer.
5. Confidential information includes, but is not necessarily limited to:
   a. Participant/ Individual information;
   b. Business information;
   c. Financial information;
   d. Operational information; and
   e. Most personnel information.
6. If the sensitivity of the information is not readily apparent, the creator of the document may mark the document as “Help At Home Confidential” in a prominent location.

Responsibilities:

1. All Help At Home Workforce are responsible for understanding and following all security related policies and procedures related to Information Classification.
2. The Security Officer is responsible for ensuring all Help At Home Workforce understand and follow security related policies and procedures related to Information Classification.

Policy History: Initial effective date: January 1, 2016

SP27 - Network Security Policy

Purpose: The purpose of this policy is to establish standards for secure communication devices and data on equipment that is owned and/or operated by Help At Home. By securing Help At Home's network and infrastructure, Help At Home will minimize unauthorized access to the organization's proprietary information and technology.

Policy:

1. Help At Home will evaluate the need for secure communication on all networks, public and private, that are utilized to transmit Help At Home sensitive information.
2. Where secure communications are required, technology and processes will be put in place to ensure the confidentiality and integrity of sensitive information.

Procedure(s):

1. Where secure communications are required, technology and processes will be put in place to ensure the confidentiality and integrity of sensitive information.
2. The standard for network protocols in the Help At Home infrastructure is TCP/IP.
3. Help At Home will:
    a. Use encryption as much as possible to protect data;
    b. Use firewall(s) to secure critical segments;
    c. Deploy Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) on all critical segments;
    d. Disable all services that are not in use or services that have use of which you are not sure; and
    e. Use wrappers around all services to log their usage as well as to restrict connectivity.

Responsibilities:

1. The Security Officer will be responsible for ensuring that network protocols are configured securely.

Policy History: Initial effective date: January 1, 2016

SP28 - Email Security Policy

Purpose: The purpose of this policy is to protect the confidentiality and integrity of sensitive information that may be sent or received via email.

Policy: Help At Home will identify whether sensitive information is permitted to be transmitted over email, and secure all email transmissions of sensitive information whenever it is permitted.

Procedure(s):

1. Help At Home recognizes that using email without the use of an encryption mechanism is an insecure means of sending and receiving messages. Help At Home will evaluate emerging encryption solutions for email and implement them when one is found that is:
   a. Technically sound;
   b. Reasonable to implement and use by workforce members, and
   c. Financially reasonable.
2. **Guidelines for Sending Sensitive Information via Email.** Until a workable encryption mechanism is implemented, Help At Home will utilize the following guidelines regarding sending sensitive information via email:
   a. Emails containing sensitive information are permitted only when both the sender and receiver are members of Help At Home's workforce and the email stays within the confines of Help At Home's local network. That is, both email addresses must end with "Help At Home.us."
   b. When sending sensitive information via email, care should be taken to send only the minimum necessary.
   c. Electronic information about a participant/ individual, in an organized set of records, should be protected to the extent that a hard copy record is protected, and disclosed only when required for authorized purposes.
3. **General Email Requirements**
   a. Help At Home email systems are intended for official and authorized purposes only.
   b. Help At Home considers email messages to be company property. Therefore, email equipment operated by or for Help At Home Workforce are subject to the same restrictions on their use as any other company-furnished resource provided for use by members of the workforce.
   c. Employees must use the Help At Home email system for all official email correspondence.
   d. Employees should have no expectation of privacy in the use of the email system.
4. **General Guidance about Email.** Every email transmitted by an individual reflects on the organization's credibility and the professionalism of the writer. Adherence to the basic rules of Help At Home "netiquette" below will alleviate problems and help cast you and Help At Home in a favorable light.
   a. Beware of hidden readers. **If confidentiality is an issue, do not use email. You may intend** to send a message to one person, but an inaccurate keystroke could land the email on dozens or hundreds of readers' screens.
   b. **Write as though mom were reading**. Do not take email too casually. Write your message as if your Director, the media or your mom were reading it.

c. **Keep all the organization’s policies in mind**. A policy is a policy. You are obligated to adhere to the organization’s policies, whether working on Help At Home provided tools or off site on personal tools.

d. **Do not take the chance of sending a hastily written email that could worsen an already difficult decision**.

e. **Control the urge to flame.** An email flame is a message that is hostile, blunt, rude, insensitive, or obscene. Flames and the obscene and abusive language that feed them have no place at Help At Home.

f. **Respect others’ time.** Do not use the organizational system to send or forward spam, non-business related messages, or personal correspondence.

g. **Never reply to spam.** If you are on the receiving end of spam, do not reply to the “unsubscribe” option. Your reply merely confirms your email address and encourages the sender to sell your address to other spammers.

h. **Do not post your business email address on a personal website**. Spambots automatically search the web for email addresses for use by spammers.

i. **Do not email to the world.** Send emails only to readers with a legitimate need for the information. Mail to group list only when it is appropriate for everyone on the list to receive the message. Staff is prohibited from sending organizational-wide email messages to all staff without prior approval of the individual’s Director, and/or IT. If you do not wish a message to be forwarded once received, put that in the email so the recipient is aware.

j. **Copy with care**. Sending a courtesy copy (CC) or blind courtesy copy (BCC) to a recipient who does not need to read your message wastes everyone’s time.

k. **Do not oversell your message.** Reserve the urgent classification for messages that demand immediate attention.

l. **Ask permission to forward material**. Avoid infringement on copyright laws on publications to which you may subscribe. Seek authorization from the original sender before sending out material.

m. **Consider email limitations.** Email may be the best way to deliver a message quickly but is not necessarily the best route to a quick reply. For an immediate response to a pressing issue don’t rely on email. Instead, pick up the phone or schedule a face-to-face meeting.

n. **Know who sees your message**. Remember that when you post something on a friend’s Facebook page, you are sending it to all of their friends as well. There are few-to-no boundaries in this type of activity.

5. Authorized Access to Email Messages

a. Email system administrators and others with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate Help At Home management officials. However, Help At Home officials will have access to email messages whenever there is a legitimate purpose for such access, e.g., technical or administrative problems.

b. When email is not in use, users are to exit the software to prevent unauthorized access.

Responsibilities:

1. All Help At Home Workforce are responsible for abiding by the terms and guidelines set forth by this policy.

2. The Security Officer is responsible for:

   a. Evaluating, on a periodic basis, emerging encryption solutions for email and implementing them when one is found the meets the criteria described in the policy section of this document.

   b. Maintaining procedures and forms in support of this policy.

   c. Monitoring and enforcing workforce compliance with this policy.

Policy History: Initial effective date: January 1, 2016

SP29 - Remote Access Policy

Purpose: The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to Help At Home's enterprise infrastructure to a reasonable and appropriate level.

Policy: Help At Home will take all reasonable and appropriate steps to ensure the secure and authorized use of all remote access capabilities and solutions.

Procedure(s): The Help At Home remote access infrastructure must follow these guidelines:

1. It is the responsibility of Help At Home employees, contractors, vendors and agents with remote access privileges to Help At Home corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Help At Home.
2. General access to the Internet for recreational use by immediate household members through the Help At Home network on personal computers is permitted for employees that have flat-rate services.
    a. The Help At Home Workforce is responsible to ensure the family member does not violate any Help At Home policies, does not perform illegal activities, and does not use the access for outside business interests; and
    b. The Help At Home Workforce bears responsibility for the consequences should he or she misuse the access.
3. Secure remote access must be strictly controlled. Control will be enforced by using strong passwords. Please refer the Password Management Policy.
4. At no time should any Help At Home Workforce provide their login or email password to anyone, not even family members.
5. Help At Home Workforce and contractors with remote access privileges must ensure that their Help At Home-owned or personal computer or workstation, which is remotely connected to Help At Home corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
6. Help At Home Workforce and contractors with remote access privileges to Help At Home's corporate network must not use non-Help At Home email accounts (for example, Gmail, Yahoo, AOL, and Outlook), or other external resources to conduct Help At Home business, thereby ensuring that official business is never confused with personal business.
7. Routers for dedicated ISDN lines configured for access to the Help At Home network must meet minimum authentication requirements of CHAP.
8. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
9. Frame Relay must meet minimum authentication requirements of DLCI standards.
10. Non-standard hardware configurations must be approved by the Security Officer.
11. All hosts that are connected to Help At Home internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.
12. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Help At Home production network must obtain prior approval from the Security Officer.

Responsibilities:

1. The Security Officer is responsible for:

a. Ensuring that all remote access connections are used in accordance with policy requirements;

b. Reviewing related log files from key systems on a regular basis; and

c. Sending reminders to all employees about remote access security.

Policy History: Initial effective date: January 1, 2016

SP30 - Portable Mobile Devices Policy

Purpose: The purpose is to secure the use of portable devices used by members of the workforce.

Policy:

1. Help At Home will ensure that wherever and whenever the use of portable devices is deemed necessary, these devices will be appropriately secured and used only by properly authorized members of the workforce.
2. Help At Home will ensure that all portable devices will be used according to the guidelines defined in this policy.

Procedure(s):

1. Confidential or sensitive data must be accessed only on server systems.
2. Sensitive information may only be stored on portable systems if appropriate encryption software authorized by the IT department is installed on the device.
3. Any information stored on the portable system must be saved only in those folders that keep information encrypted.
4. Strong password controls must be implemented for all users of portable devices. This includes requirements for minimal password length and frequency of password changes. Please refer the Password Management Policy.
5. When working on portable devices from a remote location, including from home, only secure connections must be used to access sensitive information. If wireless communication is used with portable devices, then the device must be configured as defined by the IT department to ensure use of secure protocols. Please refer to the Remote Access Policy.
6. Backups of information from portable devices must be conducted regularly and stored securely.
7. Employees must logoff and shut down portable devices with sensitive data before leaving the work space.
8. Protection against malicious software should be installed and be kept up to date on portable devices.
9. Devices must be configured to automatically logoff users according to the Automatic Logoff Policy.
10. Portable devices must not be left unattended. When not in use, portable devices should be locked away or special locks should be used to secure the equipment.

Responsibilities:

1. Members of the workforce are responsible for:
    a. The security of portable devices they use for work; and
    b. Taking special care to ensure that sensitive information is not compromised.
2. The Security Officer is responsible for:
    a. Ensuring that key elements of this policy are included in annual training provided to all members of the workforce;
    b. Including elements of this policy as security reminders sent to members of the workforce;
    c. Training members of the workforce on any encryption software or password controls that are installed or implemented on portable devices; and

d. Conducting random audits of portable systems to check for unauthorized or unsecured files.

Policy History: Initial effective date: January 1, 2016

SP31 - Wireless Security Policy

Purpose: The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of Help At Home's wireless infrastructure to a reasonable and appropriate level.

Policy:

1. Help At Home will operate all wireless networks in a secure manner so as to ensure the confidentiality, integrity, and availability of all sensitive information transmitted over wireless networks.
2. Help At Home will ensure that all wireless devices are configured and operated according to the requirements set forth in this policy.

Procedure(s): Help At Home wireless infrastructure must comply with the following guidelines:

1. **Design**
   a. Configure a firewall between the wireless network and the wired infrastructure.
   b. Ensure that 128-bit or higher encryption is used for all wireless communication.
   c. Fully test and deploy software patches and updates on a regular basis.
   d. Deploy Intrusion Detection Systems (IDS) on the wireless network to report suspected activities.
2. **Access Points (AP)**
   a. Maintain and update an inventory of all Access Points (AP) and wireless devices.
   b. Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
   c. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
   d. The default settings on APs, such as those for SSIDs, must be changed.
   e. APs must be restored to the latest security settings when the reset functions are used.
   f. Ensure that all APs have strong administrative passwords.
   g. Enable user authentication mechanisms for the management interfaces of the AP.
   h. Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
   i. Turn on audit capabilities on AP; review log files on a regular basis.
3. **Mobile Systems**
   a. Install anti-virus software on all wireless clients.
   b. Install personal firewall software on all wireless clients.
   c. Disable file sharing between wireless clients.

Responsibilities:

1. The Security Officer is responsible for:
   a. Ensuring that all wireless end systems, such as laptops, PDAs, smartphones and APs, are deployed based on policy requirements.
   b. Reviewing log files from APs and other systems on a regular basis.
   c. Sending reminders to all Help At Home Workforce about wireless network security.

Policy History: Initial effective date: January 1, 2016

SP32 - Data Breach Management

Purpose: The purpose is to provide guidance on decisions made and actions taken following the identification of a data breach. This policy is designed to minimize the loss and destruction of data, mitigate the weakness that was exploited, and restore all computing and other impacted services to Help At Home.

Policy: Help At Home will ensure that if a data breach is discovered the steps laid out in this policy will be followed in order to prevent further damage, assess the severity of the breach, and manage all breach-related activities.

Procedure(s): If a data breach is discovered at Help At Home, the following steps will be followed in order to prevent further damage, assess the severity of the breach, and manage all associated breach-related activities.

1. Once a breach has been identified the Security Officer will:
    a. Assemble the Security Incident Response Team (SIRT) according to the Security Incident Procedures Policy;
    b. The SIRT will conduct a risk assessment. The assessment will consider at least the following factors:
        i. the nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
        ii. the unauthorized person who used the protected health information or to whom the disclosure was made;
        iii. whether the protected health information was actually acquired or viewed; and
        iv. the extent to which the risk to the protected health information has been mitigated.
    c. Develop a response according to the Response and Reporting Policy;
    d. Review the breach details and develop an appropriate response to prevent further data leakage; and
    e. Assess the details of the breach.
2. The Security Officer and the SIRT will manage all phases of the process once a breach has been identified.
3. The Security Officer and the SIRT will keep Help At Home leadership apprised of the situation.
4. Priorities of the Security Officer and the SIRT will be:
    a. Stopping the data leakage
    b. Mitigation of the weakness that was exploited
    c. Restoration of normal business
    d. Notification of persons and businesses impacted as deemed appropriate
5. The Security Officer and SIRT will work with Help At Home legal counsel to determine applicable state and federal laws that may be applicable to the incident; including by not limited to HIPAA, HITECH, and state breach notification laws.
6. If any form of protected information is at risk then the Security Officer and SIRT are to enact the Breach Notification Policy.

7. Forensic analysis of the breach is to begin immediately upon determination of the breach, unless law enforcement deems a delay is appropriate, or additional forensic support is required beyond the Help At Home IT Team.

8. All meeting minutes, technical documentation, and hand written notes of the breach are to be compiled by the Security Officer or designee within 72 hours of the closure of the breach.

9. Any systems that were compromised or targeted as part of an incident resulting in an investigation may be quarantined as determined by the Security Officer and SIRT.

10. Based upon the scope of the perceived threat the Security Officer and SIRT will notify local law enforcement, the FBI Cyber Security Team, or the FBI Internet Crime Complaint Center (IC3).

    a. FBI Cyber Security Team: http://www.fbi.gov/contact/fo/fo.htm

    b. FBI Internet Crime Complaint Center (IC3): http://www.ic3.gov/default.aspx.

Responsibilities:

1. The Security Incident Response Team (SIRT) is responsible for the proper management of the security incident

2. All workforce members are responsible for understanding and following all policies and procedures related to data breaches.

3. The Security Officer is responsible for ensuring all workforce members understand and follow policies and procedures related to security breaches.

Policy History: Initial effective date: January 1, 2016

SP33 - Data Breach Notification

Purpose: The purpose is to provide guidance on the notification actions required following the discovery of a breach of protected information.

Policy: Help At Home will notify persons and organizations that have been impacted by a data breach. Breach notification is necessary in all situations except those in which the covered entity or business associate, as applicable, demonstrates, through a risk assessment, that there is a low probability that the PHI has been compromised (or one of the other exceptions to the definition of breach applies).

Procedure(s): Help At Home will notify persons and organization that have been impacted by a data breach.

1. The Security Officer will work with Help At Home legal counsel to determine state and federal laws that may be applicable to the incident; including but not limited to HIPAA, HITECH, and state breach notification regulations
2. Help At Home has the burden of proof for showing why breach notification was not required. Accordingly, Help At Home must document why the impermissible use or disclosure falls under one of the exceptions under Section 164.402.
3. The Security Officer will notify the marketing and communications department of Help At Home prior to any public notices
4. Notifications will be made in the most expedient time possible and without unreasonable delay
5. Notifications are to occur according to the requirements of HITECH Act for breaches of protected health information (no later than 60 calendar days from the discovery of the breach) or applicable state breach laws for protected health information.
6. The time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule.
7. Notifications may be delayed at the request of law enforcement agencies as part of their investigation process
8. Notifications may be delayed to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the impacted systems
9. Notifications will be made at no charge to the impacted participant/ individuals or organizations
10. Method(s) of notification may vary according to the type of breach, severity of breach, and applicable laws and regulations therefore;
11. All breach notifications will be made according to HITECH standards; unless state regulations set more rigorous requirements. (ARRA – Sec 13402 – Notification in the Case of a Breach)
    a. HITECH requires covered entities to notify participant/ individuals whose unsecured information has been breached within 60 days of discovery
    b. HITECH requires written notification to affected participant/ individuals by mail and if urgent, by telephone.
    c. HITECH requires business associates to notify covered entities about breaches.
    d. HITECH requires a conspicuous posting of the breach on the home page of the covered entity involved as determined by the Secretary of the Department of Health and Human Services (HHS) or in major print or broadcast media
    e. HITECH requires breaches of over 500 affected participant/ individuals to be reported to media outlets and the Secretary of HHS.

f. HITECH requires breaches of less than 500 affected participant/ individuals to be submitted as part of an annual breach log to the Secretary of HHS.

Responsibilities:

1. All workforce members are responsible for understanding and following all policies and procedures related to data breaches.
2. The Security Officer is responsible for ensuring all workforce members understand and follow all policies and procedures related to data breaches.

Policy History: Initial effective date: January 1, 2016