System Access Policy

Access to Marketware, Inc. systems & application is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, & any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems. These safeguards have been established to address the HIPAA Security regulations including the following:

Applicable Standards from the HITRUST Common Security Framework

- 01.d - User Password Management
- 01.f - Password Use
- 01.r - Password Management System
- 01.a - Access Control Policy
- 01.b - User Registration
- 01.h - Clear Desk & Clear Screen Policy
- 01.j - User Authentication for External Connections
- 01.q - User Identification & Authentication
- 01.v - Information Access Restriction
- 02.i - Removal of Access Rights
- 06.e - Prevention of Misuse of Information Assets

Applicable Standards from the HIPAA Security Rule

- 164.308a4iiC Access Establishment & Modification
- 164.308a3iiB Workforce Clearance Procedures
- 164.308a4iiB Access Authorization
- 164.312d Person or Entity Authentication
- 164.312a2i Unique User Identification
- 164.308a5iiD Password Management
- 164.312a2iii Automatic Logoff
- 164.310b Workstation Use
- 164.310c Workstation Security
- 164.308a3iiC Termination Procedure

Access Establishment & Modification

- Requests for access to Marketware, Inc. Platform systems & applications is made formally to the VP of Engineering, VP of Business Intelligence, Privacy Officer, or Security Officer.
- Access is not granted until receipt, review, & approval by the Marketware, Inc. Security Officer;
- The request for access is retained for future reference.
- All access to Marketware, Inc. systems & services are reviewed & updated on a bi-annual basis to assure proper authorizations are in place commensurate with job functions.

- Any Marketware, Inc. workforce member can request change of access.
- Access to systems is controlled using centralized user management & authentication.
- Temporary accounts are not used unless absolutely necessary for business purposes.
- Accounts are reviewed every 90 days to assure temporary accounts are not left unnecessarily.
- Accounts that are inactive for over 90 days are removed.
- Privileged users must first access systems using standard, unique user accounts before switching to privileged users & performing privileged tasks.
- All application to application communication using service accounts is restricted & not permitted unless absolutely needed. Automated tools are used to limit account access across applications & systems.
- Generic accounts are not allowed on Marketware, Inc. systems.
- Access is granted through encrypted, VPN tunnels.
- VPN utilizes AES 256 bit encryption.
- In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security & Privacy Officer to limit access & reduce risk of unauthorized access.
- Direct system to system, system to application, & application to application authentication & authorization are limited & controlled to restrict access.

Workforce Clearance Procedures

- The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification &/or to a user needing access to carry out treatment, payment, or healthcare operations.
- All access requests are treated on a 'least-access principle".
- Marketware, Inc. maintains a minimum necessary approach to access to Customer data. As such, Marketware, Inc., including all workforce members, does not readily have access to any ePHI.

Access Authorization

- Role based access categories for each Marketware, Inc. system & application are pre-approved by the Security Officer, VP of Business Intelligence or VP of Engineering.
- Marketware, Inc. utilizes hardware & software firewalls to segment data, prevent unauthorized access, & monitor traffic for denial of service attacks.

Person or Entity Authentication

- Each workforce member has & uses a unique user ID & password that identifies him/her as the user of the information system.
- Each Customer & Partner has & uses a unique user ID & password that identifies him/her as the user of the information system.

Unique User Identification

- Access to the Marketware, Inc. Platform systems & applications is controlled by requiring unique User Login ID's & passwords for each individual user & developer.
- Passwords requirements mandate strong password controls (see below).
- Passwords are not displayed at any time & are not transmitted or stored in plain text.
- Default accounts on all production systems, including root, are disabled.
- Shared accounts are not allowed within Marketware, Inc. systems or networks.

Automatic Logoff

- Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
- Information systems automatically log users off the systems after 10 minutes of inactivity.
- The Security Officer pre-approves exceptions to automatic log off requirements.

Employee Workstation Use

All workstations at Marketware, Inc. are company owned.

- Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
- Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization's system.
- Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
- Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.

- Transmitted messages may not contain material that criticizes organization, its providers, its partners, its employees, or others.
- Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
- Workstation hard drives will be encrypted using FileVault 2.0.
- All workstations have firewalls enabled to prevent unauthorized access unless explicitly granted.
- All workstations are to have the following messages added to the lock screen & login screen: *This computer is owned by Marketware, Inc., Inc. By logging in, unlocking, &/or using this computer you acknowledge you have seen, & follow, these policies (https://Marketware.com/policy/) & have completed this training new employee training. Please contact us if you have problems with this - privacy@Marketware.com.*

Wireless Access Use

- Marketware, Inc. production systems are not accessible directly over wireless channels.
- Wireless access disabled on all production systems.
- When access production systems via remote wireless connections, the same system access policies & procedures apply to wireless as all other connections, including wired.
- Wireless networks managed within Marketware, Inc. non-production facilities (offices, etc) are secured with the following configurations:
- All data in transit over wireless is encrypted using WPA2 encryption;
- SSIDs are not broadcast;
- Passwords are rotated on a regular basis, presently quarterly. This process is managed by the Marketware, Inc. Security Officer.

Employee Termination Procedures

- Supervisors are required to notify the Security Officer upon completion &/or termination of access needs & facilitating completion of the "Employee Offboarding Checklist".
- The Human Resources Department, users, & supervisors are required to notify the IS Help Desk to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report & is filed with the Privacy Officer):
- The user has been using their access rights inappropriately;
- A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
- An unauthorized individual is utilizing a user's User Login ID & password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID & password).

- The Security Officer will terminate users' access rights immediately upon notification.
- The Security Officer audits & may terminate access of users that have not logged into organization's information systems/applications for an extended period of time.

Paper Records

Marketware, Inc. does not use paper records for any sensitive information. Use of paper for recording & storing sensitive data is against Marketware, Inc. policies.

Password Management

- User IDs & passwords are used to control access to Marketware, Inc. systems & may not be disclosed to anyone for any reason.
- Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID & password.
- On all production systems & application in the Marketware, Inc. environment, password configurations are set to require that passwords are a minimum of 8 character length, account lockout after 5 invalid attempts, & account lockout after (default 20 minutes, admin configurable in app up to 60 minutes) minutes of inactivity.
- All application passwords are hashed by concatenating the user's password & a random 256-bit salt value, generated on a per-user basis, & then applying SHA-256 to the value to create a password hash. The password hash & the salt are then stored in the backend database & are used for password validation on future user authentication attempts.
- Passwords are inactivated immediately upon an employee's termination (refer to the termination procedures in this policy).
- All default system, application, & Partner passwords are changed before deployment to production.
- Upon initial login, users must change any passwords that were automatically generated for them.
- All passwords used in configuration scripts are secured & encrypted.
- If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security Office.

Customer Access to Systems

In the case of data migration, Marketware, Inc. does support customers in importing data. Marketware, Inc. obtains data from customer via sFTP v6 using AES256 bit encryption assuring all data is secured & encrypted in transit.

In the case of an investigation, Marketware, Inc. will assist customers, at Marketware, Inc.'s discretion, & law enforcement in forensics.