Roles Policy

Marketware, Inc. has a Security Officer [164.308(a)(2)] and Privacy Officer [164.308(a)(2)] appointed to assist in maintaining and enforcing safeguards towards compliance. The responsibilities associated with these roles are outlined below.

Applicable Standards from the HITRUST Common Security Framework

- 02.f - Disciplinary Process
- 06.d - Data Protection and Privacy of Covered Information
- 06.f - Prevention of Misuse of Information Assets
- 06.g - Compliance with Security Policies and Standards

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(2) - Assigned Security Responsibility
- 164.308(a)(5)(i) - Security Awareness and Training

Privacy Officer

The Privacy Officer is responsible for assisting with compliance and security training for workforce members, assuring organization remains in compliance with evolving compliance rules, and helping the Security Officer in his responsibilities.

- Provides annual training to all workforce members of established policies and procedures as necessary and appropriate to carry out their job functions, and documents the training provided.
- Assists in the administration and oversight of business associate agreements.
- Manage relationships with customers and partners as those relationships affect security and compliance of ePHI.
- Assist Security Officer as needed.

The current Marketware, Inc. Privacy Officer is Benjamin S Bartel (ben@marketware.com).

Workforce Training Responsibilities

- The Privacy Officer facilitates the training of all workforce members as follows:
- New workforce members within their first month of employment;
- Existing workforce members annually;
- Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;
- Existing workforce members as needed due to changes in security and risk posture of Marketware, Inc.
- The Security Officer or designee maintains documentation of the training session materials and attendees for a minimum of six years.
- The training session focuses on, but is not limited to, the following subjects defined in Marketware, Inc. ‘s security policies and procedures:
- HIPAA Privacy, Security, and Breach notification rules;
- HITRUST Common Security Framework;
- NIST Security Rules;
- Risk Management procedures and documentation;
- Auditing. Marketware, Inc. may monitor access and activities of all users;
- Workstations may only be used to perform assigned job responsibilities;
- Users may not download software onto Marketware, Inc.’s workstations and/or systems without prior approval from the Security Officer;
- Users are required to report malicious software to the Security Officer immediately;

- Users are required to report unauthorized attempts, uses of, and theft of Marketware, Inc.'s systems and/or workstations;
- Users are required to report unauthorized access to facilities
- Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation;
- Users may not alter ePHI maintained in a database, unless authorized to do so by a Marketware, Inc. Customer;
- Users are required to understand their role in Marketware, Inc.'s contingency plan;
- Users may not share their user names nor passwords with anyone;
- Requirements for users to create and change passwords;
- Users must set all applications that contain or transmit ePHI to automatically log off after "X" minutes of inactivity;
- Supervisors are required to report terminations of workforce members and other outside users;
- Supervisors are required to report a change in a users title, role, department, and/or location;
- Procedures to backup ePHI;
- Procedures to move and record movement of hardware and electronic media containing ePHI;
- Procedures to dispose of discs, CDs, hard drives, and other media containing ePHI;
- Procedures to re-use electronic media containing ePHI;
- SSH key and sensitive document encryption procedures.

Security Officer

The Security Officer is responsible for facilitating the training and supervision of all workforce members [164.308(a)(3)(ii)(A) and 164.308(a)(5)(ii)(A)], investigation and sanctioning of any

workforce member that is in violation of Marketware, Inc. security policies and non-compliance with the security regulations [164.308(a)(1)(ii)©], and writing, implementing, and maintaining all polices, procedures, and documentation related to efforts toward security and compliance [164.316(a-b)].

The current Marketware, Inc. Security Officer is Benjamin S Bartel (ben@marketware.com).

Organizational Responsibilities

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Marketware, Inc.'s efforts to be compliant with the HIPAA Security Regulations, HITRUST CSF, and any other security and compliance frameworks. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of ePHI. These organizational responsibilities include, but are not limited to the following:

- Oversees and enforces all activities necessary to maintain compliance and verifies the activities are in alignment with the requirements.
- Helps to established and maintain written policies and procedures to comply with the Security rule and maintains them for six years from the date of creation or date it was last in effect, whichever is later.
- Updates policies and procedures as necessary and appropriate to maintain compliance and maintains changes made for six years from the date of creation or date it was last in effect, whichever is later.
- Facilitates audits to validate compliance efforts throughout the organization.
- Documents all activities and assessments completed to maintain compliance and maintains documentation for six years from the date of creation or date it was last in effect, whichever is later.
- Provides copies of the policies and procedures to management, customers, and partners, and has them available to review by all other workforce members to which they apply.

- Annually, and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security and risk posture of ePHI stored, transmitted, or processed within Marketware, Inc. infrastructure.
- Develops and provides periodic security updates and reminder communications for all workforce members.
- Implements procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.
- Maintains a program promoting workforce members to report non-compliance with policies and procedures.
- Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
- Applies consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Marketware, Inc.
- Mitigates, to the extent practicable, any harmful effect known to Marketware, Inc. of a use or disclosure of ePHI in violation of Marketware, Inc.'s policies and procedures, even if effect is the result of actions of Marketware, Inc. business associates, customers, and/or partners.
- Reports security efforts and incidents to administration immediately upon discovery. Responsibilities in the case of a known ePHI breach are documented in the Marketware, Inc. Breach Policy.
- The Security Officer facilitates the communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
- Latest malicious software or virus alerts;
- Marketware, Inc.'s requirement to report unauthorized attempts to access ePHI;
- Changes in creating or changing passwords;

- Additional security-focused training is provided to all workforce members by the Security Officer. This training includes, but is not limited to:
- Data backup plans;
- System auditing procedures;
- Redundancy procedures;
- Contingency plans;
- Virus protection;
- Patch management;
- Media Disposal and/or Re-use;
- Documentation requirements.

Supervision of Workforce Responsibilities

Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining compliance, it is the responsibility of all workforce members (i.e. team leaders, supervisors, managers, directors, co-workers, etc.) to supervise all workforce members and any other user of Marketware, Inc.'s systems, applications, servers, workstations, etc. that contain ePHI.

- Monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
- Assist the Security and Privacy Officers to ensure appropriate role-based access is provided to all users.
- Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and Marketware, Inc.'s security policies and procedures.

Sanctions of Workforce Responsibilities

All workforce members report non-compliance of Marketware, Inc.'s policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

- The Security Officer promptly facilitates a thorough investigation of all reported violations of Marketware, Inc.'s security policies and procedures. The Security Officer may request the assistance from others.
- Complete an audit trail/log to identify and verify the violation and sequence of events.
- Interview any individual that may be aware of or involved in the incident.
- All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
- Provide individuals suspected of non-compliance of the Security rule and/or Marketware, Inc.'s policies and procedures the opportunity to explain their actions.
- The investigator thoroughly documents the investigation as the investigation occurs.
- Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
- A violation resulting in a breach of confidentiality (i.e. release of PHI to an unauthorized individual), change of the integrity of any ePHI, or inability to access any ePHI by other users, requires immediate termination of the workforce member from Marketware, Inc.

- The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).
- In the case of an insider threat, the Security Officer and Privacy Officer are to setup a team to investigate and mitigate the risk of insider malicious activity. Marketware, Inc. workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.
- The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.