Auditing Policies

Responsibility for auditing information system access and activity is assigned to Marketware, Inc.'s Security Officer. The Security Officer shall:

- Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
- Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
- Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes, report formats, evaluation, follow-up, etc.).
- All connections to Marketware, Inc. are monitored. Access is limited to certain services, ports, and destinations. Exceptions to these rules, if created, are reviewed on an annual basis.
- Marketware, Inc.'s auditing processes shall address access and activity at the following levels listed below. In the case of PaaS Customers, Application and User level auditing is the responsibility of the Customer; Marketware, Inc. provides software to aggregate and view User and Application logs, but the log data collected is the responsibility of the PaaS Customer. Auditing processes may address date and time of each log-on attempt, date and time of each log-off attempt, devices used, functions performed, etc.
- User: User level audit trails generally monitor and log all commands directly initiated by the user, all identification and authentication attempts, and data and services accessed.
- Application: Application level audit trails generally monitor and log all user activities, including data accessed and modified and specific actions.

- System: System level audit trails generally monitor and log user activities, applications accessed, and other system defined specific actions. Marketware, Inc. utilizes file system monitoring from OSSEC to assure the integrity of file system data.

- Network: Network level audit trails generally monitor information on what is operating, penetrations, and vulnerabilities.

- Marketware, Inc. shall log all incoming and outgoing traffic to into and out of its environment. This includes all successful and failed attempts at data access and editing. Data associated with this data will include origin, destination, time, and other relevant details that are available to Marketware, Inc..

- Marketware, Inc. utilizes OSSEC to scan all systems for malicious and unauthorized software every 2 hours and at reboot of systems. Alerts from OSSEC are sent to Kibana, the centralized logging service that we use.

- Marketware, Inc. leverages process monitoring tools throughout its environment.

- Marketware, Inc. treats its Developer Portal as a Platform Add-on and, as such, it logs all activity associated with Developer Portal Access.

- Marketware, Inc. uses OSSEC to monitor the integrity of log files by utilizing OSSEC System Integrity Checking capabilities.

- Marketware, Inc. shall identify “trigger events” or criteria that raise awareness of questionable conditions of viewing of confidential information. The “events” may be applied to the entire Marketware, Inc. Platform or may be specific to a Customer, partner, business associate, Platform Add-on or application (See Listing of Potential Trigger Events below).

- In addition to trigger events, Marketware, Inc. utilizes OSSEC log correlation functionality to proactively identify and enable alerts based on log data.

- Logs are reviewed weekly by Security Officer.

- Marketware, Inc.'s Security Officer and Privacy Officer are authorized to select and use auditing tools that are designed to detect network vulnerabilities and intrusions. Such tools are explicitly prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:
- Scanning tools and devices;
- Password cracking utilities;
- Network "sniffers."
- Passive and active intrusion detection systems.
- The process for review of audit logs, trails, and reports shall include:
- Description of the activity as well as rationale for performing the audit.
- Identification of which Marketware, Inc. workforce members will be responsible for review (workforce members shall not review audit logs that pertain to their own system activity).
- Frequency of the auditing process.
- Determination of significant events requiring further review and follow-up.
- Identification of appropriate reporting channels for audit results and required follow-up.
- Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.
- Testing may be carried out internally or provided through an external third-party vendor. Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services - separation of duties).
- Testing shall be done on a routine basis, currently monthly.

- Software patches and updates will be applied to all systems in a timely manner. In the case of routine updates, they will be applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within 30 days from testing and all security patches are applied within 90 days after testing.

- In the case of PaaS Customers, updates to Application and Database versions are the responsibility of Customers, though Marketware, Inc. will, at its own discretion, notify and recommend updates to customer systems.

Audit Requests

- A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, Security Officer, Customer, Partner, or an Application owner or application user.

- A request for an audit for specific cause must include time frame, frequency, and nature of the request. The request must be reviewed and approved by Marketware, Inc.'s Privacy or Security Officer.

- A request for an audit must be approved by Marketware, Inc.'s Privacy Officer and/or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.

- Should the audit disclose that a workforce member has accessed ePHI inappropriately, the minimum necessary/least privileged information shall be shared with Marketware, Inc.'s Security Officer to determine appropriate sanction/ corrective disciplinary action.

- Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by Marketware, Inc.'s Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that Marketware, Inc. consider seeking risk management and/or legal counsel.

Review and Reporting of Audit Findings

- Audit information that is routinely gathered must be reviewed in a timely manner, currently monthly, by the responsible workforce member(s).
- On a quarterly basis, logs are reviewed to assure the proper data is being captured and retained.
- The reporting process shall allow for meaningful communication of the audit findings to those workforce members, Customers, or Partners requesting the audit.
- Significant findings shall be reported immediately in a written format. Marketware, Inc.'s security incident response form may be utilized to report a single event.
- Routine findings shall be reported to the sponsoring leadership structure in a written report format.
- Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
- Security audits constitute an internal, confidential monitoring practice that may be included in Marketware, Inc.'s performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable e PHI shall not be included in the reports).
- Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.

Auditing Customer and Partner Activity

- Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between Marketware, Inc. and the 3rd party. Marketware, Inc. will make every effort to assure Customers and Partners do not gain access to data outside of their own Environments.

- If it is determined that the Customer or Partner has exceeded the scope of access privileges, Marketware, Inc.'s leadership must remedy the problem immediately.
- If it is determined that a Customer or Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, Marketware, Inc. must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

Audit Log Security Controls and Backup

- Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.
- All audit logs are encrypted in transit and at rest to control access to the content of the logs.
- Audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges. This is done to apply the security principle of "separation of duties" to protect audit trails from hackers.
- For PaaS Customers choosing to use Marketware, Inc. logging services, log data will be separated from the log data of other Marketware, Inc. Customers.

Workforce Training, Education, Awareness and Responsibilities

- Marketware, Inc. workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and ePHI. Marketware, Inc.'s commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. Marketware, Inc. workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.

- Marketware, Inc. Customers are provided with necessary information to understand Marketware, Inc. auditing capabilities, and PaaS Customers can choose the level of logging and auditing that Marketware, Inc. will implement on their behalf.

External Audits of Information Access and Activity

- Prior to contracting with an external audit firm, Marketware, Inc. shall:
- Outline the audit responsibility, authority, and accountability;
- Choose an audit firm that is independent of other organizational operations;
- Ensure technical competence of the audit firm staff;
- Require the audit firm’s adherence to applicable codes of professional ethics;
- Obtain a signed HIPAA business associate agreement;
- Assign organizational responsibility for supervision of the external audit firm.

Retention of Audit Data

- Audit logs shall be maintained based on organizational needs. There is no standard or law addressing the retention of audit log/trail information. Retention of this information shall be based on: A. Organizational history and experience. B. Available storage space.
- Reports summarizing audit activities shall be retained for a period of six years.
- Log data is currently retained and readily accessible for a 1-month period. Beyond that, log data is available via cold backup.
- For Paas Customers, they choose the length of backup retention and availability that Marketware, Inc. will implement and enforce.

Potential Trigger Events

- High risk or problem prone incidents or events.

- Business associate, customer, or partner complaints.
- Known security vulnerabilities.
- Atypical patterns of activity.
- Failed authentication attempts.
- Remote access use and activity.
- Activity post termination.
- Random audits.