Facility Access Policy

Marketware, Inc. works with Subcontractors to assure restriction of physical access to systems used as part of the Marketware, Inc. Platform. Marketware, Inc. and its Subcontractors control access to the physical buildings/facilities that house these systems/applications, or in which Marketware, Inc. workforce members operate, in accordance to the HIPAA Security Rule 164.310 and its implementation specifications. Physical Access to all of Marketware, Inc. facilities is limited to only those authorized in this policy. In an effort to safeguard ePHI from unauthorized access, tampering, and theft, access is allowed to areas only to those persons authorized to be in them and with escorts for unauthorized persons. All workforce members are responsible for reporting an incident of unauthorized visitor and/or unauthorized access to Marketware, Inc.'s facility.

Of note, Marketware, Inc. does not have ready access to ePHI, it provides cloud-based, compliant infrastructure to covered entities and business associates. Marketware, Inc. does not physically house any systems used by its Platform in Marketware, Inc. facilities. Physical security of our Platform servers is outlined here:

http://awsmedia.s3.amazonaws.com/pdf/aws_security_whitepaper.pdf

Applicable Standards from the HITRUST Common Security Framework

- 08.b - Physical Entry Controls
- 08.d - Protecting Against External and Environmental Threats
- 08.j - Equipment Maintenance
- 08.l - Secure Disposal or Re-Use of Equipment
- 09.p - Disposal of Media

Applicable Standards from the HIPAA Security Rule

- 164.310(a)(2)(ii) Facility Security Plan
- 164.310(a)(2)(iii) Access Control & Validation Procedures
- 164.310(b-c) Workstation Use & Security

Marketware, Inc.-controlled Facility Access Policies

- Visitor and third party support access is recorded and supervised. All visitors are escorted.
- Repairs are documented and the documentation is retained.

- Fire extinguishers and detectors are installed according to applicable laws and regulations.
- Maintenance is controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organizations maintenance program.
- Electronic and physical media containing covered information is securely destroyed (or the information securely removed) prior to disposal.
- The organization securely disposes media with sensitive information.
- Physical access is restricted using smart locks that track all access.
- Restricted areas and facilities are locked and when unattended (where feasible).
- Only authorized workforce members receive access to restricted areas (as determined by the Security Officer).
- Access and keys are revoked upon termination of workforce members.
- Workforce members must report a lost and/or stolen key(s) to the Security Officer.
- The Security Officer facilitates the changing of the lock(s) within 7 days of a key being reported lost/stolen
- Enforcement of Facility Access Policies
- Report violations of this policy to the restricted area's department team leader, supervisor, manager, or director, or the Privacy Officer.
- Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Marketware, Inc.
- Workstation Security
- Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities.
- All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
- All workstations purchased by Marketware, Inc. are the property of Marketware, Inc. and are distributed to users by the company.