Facility Access Policy

This policy, and associated procedures for facility access, has been sub-contracted in part to a third-party, HIPAA compliant, Platform as a Service vendor (PaaS Vendor). We have verified that their policies and procedures meet or exceed our standards and those of HIPAA and the HITRUST Common Security Framework. As such, we have assurances that facility access to both web and data servers is appropriately restricted.

Proof of such due diligence is kept by the Security Officer.

Of note, we do not have physical access to ePHI. We do not physically house any systems used by our production environment, where ePHI and other protected data reside.

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

Facility Access

We are responsible for Workstation and Workplace Security as follows:

1. Visitor and third party support access is supervised. All visitors are escorted.
2. **See System Access Policy** for how the organization manages workstations and other related equipement including enforcement of the policy.
3. **See Disposal Media Policy** for information about how the organization securely disposes media.
4. Maintenance of facilities and equipment is controlled and conducted by authorized

personnel in accordance with supplier-recommended intervals, insurance policies, and the organizations maintenance program.

5. Fire extinguishers and detectors are installed according to applicable laws and regulations.

PaaS Vendor is responsible for facilities where ePHI reside as follows:

1. Visitor and third party support access is recorded and supervised to any facility. All visitors are escorted.
2. Repairs are documented and the documentation is retained.
3. Fire extinguishers and detectors are installed according to applicable laws and regulations.
4. Maintenance of facility and equpment is controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the organizations maintenance program.
5. Electronic and physical media containing covered information is securely destroyed (or the information securely removed) prior to disposal.
6. Securely disposing of media with sensitive information.
7. 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
8. 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.