BEHAVIORAL TECH RESEARCH

CAT HIPAA Compliance

The CAT system server is hosted by Connectria Hosting. Connectria provides Health Insurance Portability and Accountability Act (HIPAA) Compliant Hosting for healthcare data and complies with all US regulations and security standards regarding the storage of Protected Health Information. More information about their facilities and security is below and can also be found on the web: www.connectria.com.

Connectria's Security Architecture: Connectria utilizes a two-tier security architecture. The first tier of the architecture is implemented by redundant perimeter firewalls, based on the Cisco Secure IOS. The firewall protects against malicious hacking attempts and Denial of Service attempts. The second tier of the security architecture is implemented by the use of private, non-routable IP address spaces. In the unlikely event the firewall is breached, the servers behind the firewall cannot route traffic to the Internet. Connectria also provides Virus Scanning, Network-based Intrusion Detection, and Server-based Intrusion detection as part of our Enhanced Hosting Services, at additional costs.

Awareness: Connectria monitors multiple channels of information in order to stay atop of the ever-changing security environment. Some of the sources utilized include CERT, BugTraq, Microsoft Security Bulletins and other vendor sites. Additionally, Connectria works with our Internet Service Providers to identify and respond to security challenges on the Internet.

Physical Security: Connectria maintains physical security to our facilities by limiting access to the buildings where our data centers are housed as well as to the physical data centers within those buildings. All data centers are protected by multiple layers of security including multiple layers of electronic building & facility access secured by magnetic locks, 24/7 onsite-personnel, monitored and recorded closed-circuit television, person-traps, and mandatory identity logging of all outside visitors.

Site Electrical Power: Connectria's St. Louis Data Centers maintain three separate power feeds from Ameren. Connectria's Philadelphia Data Center maintains two separate power feeds from PECO Energy. Our data centers feature multiple power distribution units to condition the incoming electricity. Connectria data centers are protected by redundant UPS power systems to power our hosted systems. All facilities have diesel generator backup systems to protect buildings against an extended loss of commercial power. The generators are configured to automatically start when they sense a loss of power from the local electric utilities. The generators are tested monthly to ensure they are in proper working condition. Connectria takes great pride in the high availability and uptime performance of its data centers.

Fire Protection: Connectria data centers are protected from fire damage by design with concrete floors, steel ceilings, and steel framed racks. Our data centers are equipped with a combination of FM200 fire suppression and a multi-zoned, pre-action, dry-pipe system. In order for the systems to trip, multiple cross-linked events must occur. These include detection by ceiling mounted smoke-heads and sensors located throughout the facility. Lastly a sprinkler head must trip in order for the dry-pipe system to activate. This requires a temperature of 140 degrees F at the head location. Upon detection of the presence of fire or smoke in the data center, the detection and control panel will sound an alarm, shut down air handlers, disconnect power from the protected equipment, and then release the extinguishing agent(s) localized at the event point.

Email: info@btechresearch.com **Telephone**: 206-957-1044 **Fax**: 206-957-0518