HIPAA Compliance Statement

Carty Web Strategies, DBA Home Campus has put into place numerous measures to certify it is voluntarily compliant with the regulations and conditions set forth in the Security Rule of Health Insurance Portability and Availability Act of 1996 (HIPAA). Home Campus has implemented policies, processes and procedures designed to ensure compliance with Federal and State information security laws, regulations, and rules, and monitors ongoing compliance efforts and maintains several reporting tools that are required by law or requested by its customers in order to remain accountable. For those wishing to obtain more information regarding our compliance please contact Home Campus at (562)206-2486 or Support@Home-Campus.com.

Technical Safeguards

Access Control – Each user has unique username and password for identifying and tracking user identity. In the case of emergencies, we have procedures to obtain user information. The system will automatically logoff which will terminate the session after inactivity. We have SSL attached to the site (secured socket layer) which encrypts the data against hackers

Audit Controls – Software mechanisms that record and examine activity in all information systems.

Integrity – Medical information can be destroyed by the User, School Administration and Home Campus at the end of the school year when sensitive information is purged.

Authentication – Email authentication is required when seeking access to an existing account. School Admin cannot obtain user login information.

Transmission Security – Electronically transmitted medical information can only be modified through User accounts. The site, which includes medical information, is encrypted.

Physical Safeguards

Workstation Use – Home Campus admin (Currently 9 people) must login using their unique login information at any computer that accesses medical information.

Workstation Security – Home Campus offices are locked while unoccupied. Access during off hours is locked manually. Access is restricted to 8 authorized people.

Device and Media Coverage – Home Campus is a web-based program. Disposal of medical information from the server (Amazon Web Services) happens once a year. Schools can choose to save that information for their records before it is cleared from the server.

Administrative Safeguards

Security Management Process – Medical information is only managed on AthleticClearance.com by users through their unique login credentials. Implementation of risk analysis and measures to eliminate any chance for HIPAA violations. Employees that fail to comply will be terminated. Regular audits of the system, logs and activity.

Assigned Security Responsibility – Designated HIPAA Security and Privacy Officer – Lindsay Warkentin

Workforce Security – 9 Home Campus employees are authorized to access Users medical information. Any employee that does not have authorized access will be terminated if accessing medical information.

Information Access Management – Ensure that medical information is not accessed by partner organizations or subcontractors that are not authorized for access.

Security Awareness and Training – Periodically send updates and reminders about security and privacy policies to employees. Have procedures for guarding against, detecting and reporting malicious software. Procedures for creating, changing and protecting passwords.

Security Incident Procedures – Identify, document and respond to security incidents.

Contingency Plan – Accessible backups of medical information and procedures to restore lost data.

Evaluation – Perform periodic evaluations to see if any changes in business or law require changes to the Home Campus HIPAA Compliance Statement or procedures.

Business Associate Contracts and Other Arrangements – No business partners have access to sensitive information.