System Security, HIPAA and FERPA Compliance, Data Access

Data backups:

We backup the databases we host every 3 hours each day. These backups are maintained for 90 calendar days. A backup of our server is done each day. All file server backups are transmitted through our secure network. Data is stored for 7 years from the last date of entry.

MYSQL Server:

All databases are MYSQL Server. Our database servers are hosted on their own system through a designated IP address. The server hosting these database systems are not accessible from an outside network. All database servers are protected behind a network Firewall to prevent unauthorized intrusion.

HIPAA Compliance:

We have administrative, physical and technical safeguards in place to assure the confidentiality and integrity of PHI. To the best of our knowledge, our systems have followed protocol to ensure that we meet / exceed the following requirements for HIPAA:

1. Transmission Encryption
2. Backup Systems
3. Authorization security
4. Integrity
5. Storage Encryption
6. Disposal

FERPA Compliance:

Record access is limited to authorized persons only. Users may share injury information with school officials and staff members (ie: school nurse, coach) deemed to have legitimate interest. We do not disclose any student information without appropriate permission, or unless required to comply with a judicial order, lawfully issued subpoena, or other conditions specified in FERPA. We recommend institutions have photo permissions in place before users include student headshots or images in the system.

Authentication:

Our data on information entered is only accessible by the organization that entered it. Password and username access is required. Our systems ensure that passwords are encrypted as well as required to meet a minimum of ‘strong’ password creation with a mixture of characters.

Data Center Physical Security:

- Microsoft Azure Platform
- Environment controlled area
- Battery backup on each server
- Security enforcements
- Secure access to servers by authorized personnel only
- Encrypted Drives on all server systems
- Disaster Recovery Plan for all server systems

HTTPS security:

All connections to our databases use a 256-bit, AES SSL certificate from GoDaddy.com.

Data Access:

Patient / Athlete information is protected by several layers of access:

1. ATGenius™ users will be required to enter in their login credentials to access our system.
2. Users are automatically logged out after 20 minutes of inactivity to prevent unauthorized access.
3. Patient / Athlete information is only viewable by the school that creates and updates the records.
4. Any emails sent to Coaches / School Nurse (etc) are protected and sent through secure SMTP server ports with the highest security.
5. User login information is collected each time the user logs into the ATGenius™ system to track any unauthorized activity.
6. Restrictions are in place for additional users to allow for limited functionality and record access.

7. 2-Step Login Authentication option on all accounts
8. Login / IP Tracking system for all activity
9. Account Disabled after multiple failed login attempts

If you have any further questions about security, please contact brandon@bwcweb.com