CSMi CONFIDENTIAL
101 Tosca Drive
Stoughton, MA 02072 USA
(Phone) 781.297-2034
(FAX) 781.297-2039
(Web) www.csmisolutions.com

SportsWareOnLine Security Statement

This document describes CSMi's SportsWareOnLine security procedures.

HIPAA/FERPA

HIPAA (Health Insurance Portability and Accountability Act of 1996)

HIPAA regulations establish a set of national standards for the protection of certain protected health information (PHI). A major goal of the HIPAA regulations is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being.

Compliance

CSMi's procedures, our SportsWareOnLine product, and our website hosting are designed to assure HIPAA compliance and audited by an independent security firm.

For more information on HIPAA, see: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

FERPA (Family Educational Rights and Privacy Act)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Compliance

By policy, CSMi does not release any information stored in SportsWareOnLine. The only exception to this is if a school wishes to participate in an athletic injury study and actively joins the study group. In this case only non-identifiable (no athlete or school identifiable) data is used in the study. A number of such studies have been funded by the NATA and NCAA. Additionally, FERPA states data can be used for, *"Organizations conducting certain studies for or on behalf of the school"*.

For more information on FREPA, see: https://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Product Development

1. SportsWareOnLine is a Web 2.0 based-application. The majority of the application code is written in C#, a modern programming language used in wide variety of applications. The application code is served-up via the web using Microsoft's Internet Information Server (IIS) running on Windows 2008 servers. The data is archived using Microsoft SQL2008 Enterprise Edition.
2. The product development release cycle includes:
    a. Internal Code Development on local CSMi machines.
    b. Uploading to a beta site for QA testing by different CSMi developers.

c. Release to the Live Site.

3. All new feature development and bug resolution is tracked using an Online Agile Development Tool. The Code Base is maintained using source control tools (Visual Studio 2008/Team).

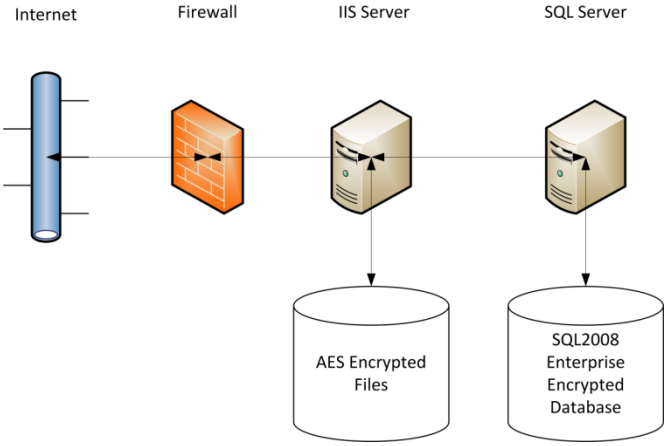
Network/Hosting Structure

Hosting

1. The application is hosted by a SSAE16 compliant hosting company (see Hosting Facility HIPAA Compliance) providing a HIPAA-compliant environment. The hosting company ensures that all systems are running properly by maintaining the physical infrastructure in a secure manner as prescribed by HIPAA guidelines as well as an SLA agreement.

Network Topology

1. The following diagram illustrates the hosting network topology.



Assets

1. The application consists of two virtual machines. The first machine runs the IIS Server and the second machine runs the SQL Database Service.

Firewall

1. The CSMi servers are isolated located behind a dedicated firewall.

IIS Server

1. The IIS server includes an internet-routable IP address.
2. Access to the CSMi application is provided via ports 80 and 443.
3. User files are encrypted using AES.

SQL Server

1. The SQL server does not have an internet-routable IP address.
2. Ports 80 and 443 are closed.
3. The SQL Database utilizes Microsoft's Transparent Data Encryption (TDE).

IIS – SQL Communication

1. The traffic between the two servers is transmitted within the hosting company via a CSMi-private (V)LAN.

Employee Screening

1. Criminal background checks are run on all CSMi employees with access to PHI.

Security Audit Reports

1. CSMi contracts with an external security firm to audit our procedures for HIPAA compliance. Additionally CSMi runs a number of intrusion tests on the SportsWareOnLine servers. Copies of the CSMi HIPAA Audit Report, Intrusion Report, and Hosting Company SSAE 16 Audit Report are available upon execution of a Non-Disclosure Agreement.

Hosting Facility HIPAA Compliance

Certifications

1. SSAE 16 (Formerly SAS 70) Audited Data Centers. Third-Party HIPAA Assessment with 100% compliance.

Domestic Hosting

1. All data is hosted within the US.

Anti-Virus Updates/OS Patches

1. Zero-day events are installed immediately. Non-critical updates are installed monthly.
2. Vulnerability Scanning For 70,000+ Vulnerabilities.
3. Managed F-Secure™ Server Antivirus Protection (Rated #1 by InfoWorld).
4. Advanced Server Hardening against 100K+ vulnerabilities.
5. Security tools perform log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. Traffic meeting the profile of intrusion traffic is null-routed or quarantined.
6. TripWire™ Server Integrity Monitoring with Auto Rollback.
7. NetZentry CleanTraffic™ Distributed Denial Of Service (DDoS) Protection.

Network Security Architecture

1. The Hosting Company 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.

Physical Security

1. The Hosting Company maintains physical security to the facilities by limiting access to the buildings where the 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.

Facility Access, Logs & Audits

1. The Hosting Company secures NOC, Meet-Me Room and other areas with electronic access controls.
2. Data Center access is restricted to their Data Center personnel only.
3. Employees who do not have data center access and other visitors are escorted under line of sight rule.
4. Access controls are user specific and updated immediately upon loss or termination of user.
5. Access logs are retained indefinitely, reviewed daily, and audited annually.

Environmental Protection

1. Pre-Action Dry-Pipe fire suppression with dual zone charging and multi-zone release.

Awareness

1. The Hosting Company 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, the Hosting Company works with their Internet Service Providers to identify and respond to security challenges on the Internet.

Tracking

1. In the event of a security notice, the Hosting Company will review the notice and determine the criticality. If the notice is deemed to present a serious threat, the work-around or patches will be immediately implemented after approval by CSMi. All notices are logged in their GWI change management and trouble ticketing system.

Data Backup

1. The Hosting company provides daily full-systems backups held for a minimum of two weeks. Data is encrypted by Hosting Company's CommVault Enterprise Class Backup System. Data is stored local on on-site disk arrays for rapid restores and held offsite on tape at their third-party storage partner.
2. CSMi independently maintains redundant off-site encrypted backups.

Recording Of Data Movements

1. The Hosting Company records data movements of electronic media both inside and outside of their facilities.

Data Destruction

1. The Hosting Company utilizes DoD Standard media wipes with 3X pass minimum. Media are destroyed with documented chain of custody upon CSMi's request.