NCFRP Child Death Review – Case Reporting System Security Information

Hardware requirements:

An internet enabled PC. Touch-screen technology has not been thoroughly tested.

Minimum software requirements:

We recommend Internet Explorer 11 or higher or Chrome. Safari is not supported. The system uses client-side java script in addition to server-side programming.

To test your system, we would be happy to set up a login to our training site, which does not contain PHI but functions the same as the production site.

As stated in the Data Use Agreement, MPHI is not responsible for any damage caused by viruses originating from any places not attributable to MPHI. It is strongly suggested that the end user have consistent/comparable security practices in place for data that is downloaded from the servers back to the end user.

Description:

The National Center for Fatality Review Case Reporting System (NFR-CRS) at MPHI is written in Microsoft .NET technologies, using the MVC and Entity frameworks, C#, and Microsoft SQL Server 2012 for the database back-end. The web servers are configured as a two node, network load balanced web farm, located in MPHI's primary data center. The servers on which the application is supported are Windows Server 2008 R2 virtual servers. The web servers are configured with dual Intel Xeon four core processors and 16GB of RAM. The database server is configured in an always-on cluster, with dual Intel Xeon six core processors and 64GB of RAM.

Data transmitted to and from the web server uses a load balancer with an integrated web application firewall. This device negotiates the best possible TLS encryption method (we do fallback to TLS < 1.2 for backwards compatibility) to enable secure, encrypted communications between MPHI servers and the site requestor. The certificate authority is GoDaddy and is renewed annually. A failover pair of stateful firewalls and intrusion prevention systems (IPSes) are utilized. The application is divided into separate web and database tiers with a stateful firewall inspecting traffic between the tiers.

For disaster recovery, the Receiver's network servers are backed-up nightly online to disk storage and replicated to disk in a second location nightly. Daily backups are kept on disk for 30 days. Data is sent to encrypted tape weekly, and weekly backups are kept off-site for 30 days. Monthly backups are saved on the encrypted backup tapes for 7 years. The tapes are delivered in locked containers via courier and stored off-site in a physically secure location.

The servers are located at the MPHI Data Center. This Data Center is a state-of-the-art facility designed from the ground up to house modern server and network infrastructure. The Center is fully capable of handling current and future high density systems and employs the latest server virtualization technologies. Some highlights of the infrastructure include:

- A location with a low risk of floods, tornados and earthquakes;
- 1000 square feet of raised floor to allow for unobstructed cooling;
- Protected by an inert gas fire suppression system and 2 hour fire walls;
- Fully equipped with secure access "prox" cards, video surveillance and a 24x7 remotely monitored fire detection and security system;
- UPS battery backup and a diesel generator on site in case of power loss; and
- Redundant communication provided via two independent Internet Service Providers using underground fiber at gigabit speeds.