Attachment 6

MPHI Child Death Review Case Reporting System – Security Information

Data transmitted to and from web servers are authenticated and encrypted with 2048-bit SSL (Secured Sockets Layer), which is the strongest currently available commercially. The certificate authority is *GoDaddy* and is renewed annually.

Two stateful firewalls are utilized, as well as intrusion detection products. The database server sits in a protected data network, with a firewall placed between the database and web server. In addition, the Child Death Review Case Reporting System server environment sits behind an F5 Load Balancer, which serves as a reverse proxy and allows for additional security protections.

The servers are in a physically secure location (located in a locked building, locked room, and locked rack) with restricted access and a complete automatic temperature alarm system and fire sprinkler protection system. The server rooms have separate air conditioning systems, and electrical supplies are backed up with uninterruptible power supplies, which are backed up by a Diesel Generator for long term power outages. When the MPHI Data Center is closed during non-business hours, the building is locked, an electronic alarm system is activated and access into the building is permitted only through the use of electronic reader cards. The MPHI Data Center is also equipped with a video surveillance system. See description of Data Center for more information.

MPHI continuously updates virus-scanning software on all servers and workstations. Critical patches are applied within 30 days of stable release from vendor. Automated monitoring via various technologies, including SCOM and Solar Winds with emailed and texted alerts, are in place. Data integrity is checked on a routine basis by both automatic and manual processes.

A small group of MPHI staff have access to the server room for server management and maintenance. These staff abide by strict confidentiality agreements. Custodial and building maintenance staff are not allowed in the server area except in the presence of MPHI staff.

MPHI staff regularly and randomly audit their database servers to ensure there are no security violations. MPHI conducts an annual security audit using enterprise tools.

For disaster recovery, the server is backed-up nightly to online disk storage, and replicated to disk in a second location nightly. Daily backups are kept on disk for 30 days. Then, the data is sent to encrypted tape weekly, and weekly backups are kept offsite for 30 days. Lastly, monthly backups are saved on the encrypted backup tapes for seven years. The tapes are delivered in locked containers via courier and stored off-site in a physically secure location.

May 2014