Imagecast system information

System Name: Imagecast & iSite

Version: 10.3.9.91 SP51 & 3.5.86.0

Brief description: Imagecast is the Radiology Information System (RIS) and iSite is the Picture Archival Communication System (PACS). The two systems share a common database.

Validation documents
System validation documents are available on site. All test scripts and testing results are located in paper copies in file cabinets and scanned document on our network shared drive.

Audit trail
There is a system generated audit trail. This is monitored at several points. Any variance is brought to the attention of security, compliance or the Imaging Systems Directory, depending on the severity of the variance.

User training documentation
Department managers maintain training documentation for their staff. The sites are also responsible for new employee training.

Controlled computer date and time
The computer date and time are controlled using NTP (network time protocol).

Complete records contained
The system contains complete records including data, audit trail, e-signature and metadata.

Agency inspection process
There is a process to copy records for agency (i.e. study sponsor or FDA) inspection. Fairview has policies to follow regarding the external disclosure of such information.

Record collection and retention practices
Electronic record collection and retention practices are consistent with and actually may exceed what study sponsors (and FDA) require per their policies as all data is retained indefinitely.

Backup, recovery and contingency procedures
There are backup, recovery and contingency procedures for data and metadata. Test restore is performed weekly and back-ups done daily. Full disaster plans are in place and reviewed annually.

Physical security and controlled environment
There are procedures and controls for physical security, ensuring a controlled environment. The data center is a secure facility and limited access is controlled by key pad and cameras. These procedures and controls are reviewed quarterly.

User access security
There are procedures and controls for user access security. User access is controlled by following a defined provisioning process that is based on the role/position of the user.

Managing and documenting system changes
There are procedures to manage and document changes to the system. All systems are required to follow a strict change management procedure. Change documentation and processes are managed in a central change management tool.

Protection from viruses, hackers, etc.

There is protection from viruses, hackers, etc. There is intrusion protection and antivirus on all systems. Operating system vulnerabilities are also monitored and patched when resolution occurs.

Device and operational checks
There are device and operational checks as appropriate. Servers are monitored for availability. Environmental conditions are checked in the server room. Operations personnel physically check servers hourly.

System documentation
The system documentation is maintained appropriately. This is a vendor application and is well documented by the vendor. Volumes of manuals, data dictionaries, processes, server connectivity, work plans, work flows, etc. are all maintained.

Electronic signatures
Electronic signatures are used.

E-signatures
E-signatures are used and there are written procedures to hold people accountable for their signature. A system-wide policy is in place that stipulates e-signature requirements and addresses violations. E-signatures include the time, date, signature and meaning of signature. This is included in the policy dictating how e-signatures are created.