The ASP Environment: Security Features

Some electronic medical record (EMR) vendors may offer EMRs hosted in and provided from a central data centre. This service is often referred to as an application service provider (ASP) environment—where data and the EMR application software is hosted offsite and not within the clinic.

The ASP environment offers several enhanced security features for patient information over those provided in stand-alone local installations. If you are considering ASP as part of your EMR, ask your vendor about the following:

Data Security – There are industry standards that should be met by the EMR vendors. Ask potential vendors if their ASP environment has been tested and meets these rigorous standards.

Data Privacy – Each physician's patient data should be maintained separately in a partitioned database. There should be no consolidation or amalgamation of patient data between physicians—unless there is a need and agreement between physicians to such sharing.

Data Encryption – All patient data being transferred between the hosted data centre and the physician's office through an open Internet connection should be encrypted to ensure privacy and security.

Access Management – Access to patient data should be controlled giving only the physician and his/her staff or designate role-based access to the data. All access to data should be recorded with the ability be audited.

Reliability/Availability – Failure in the server hardware, power and communications network should not result in a loss of service to the physician's office—there should be no "single point of failure." Vendors should also provide network and application management as part of the hosted service, as well as disaster recovery to restore service quickly following a catastrophic event or failure.

Performance Monitoring – The performance and the responsiveness of the hosted services should be monitored to ensure the highest level of service is delivered.

Data Centre Security – The data centre itself should be required to meet rigorous security requirements, including monitored and secure access to the facility, power backup, cooling and fire suppression systems, and staffing on a 24/7 basis.

This centrally-hosted service model improves overall service:

- Enhances protection and management of data
- Minimizes the need for IT infrastructure knowledge/skills at the physician's clinic
- Negates the need for expensive server upgrades or replacements
- Eliminates the requirement for regular local file backups

Protect Patient Privacy

All clinics should keep malware programs on their local systems, to check systems regularly for any potential viruses or security breaches and until the transition to the ASP environment has happened, to keep servers up to date. If there has been a security breach within a physician clinic, the following steps must be taken immediately:

- Call the EMR vendor immediately. Troubleshooting and support should be made available as soon as possible to correct the problem.
- Contact the Office of the Information and Privacy Commissioner. Document the call.

  www.oipc.ab.ca
  Phone: 780.422.6860
  Toll Free: 1.888.878.4044
  Fax: 780.422.5682
  generalinfo@oipc.ab.ca

- Contact the College of Physicians & Surgeons of Alberta for questions and concerns related to the Standards of Practice.

  www.cpsa.ab.ca
  Phone: 780.423.4764
  memberinquiries@cpsa.ab.ca

The information in this fact sheet is provided for education and guidance only and is not intended to replace expert advice. Physicians are responsible for making informed decisions to meet their medical-legal obligations.

22-Oct-13