EMR-Link System Architecture

Introduction
This document describes the system architecture of EMR-Link, for purposes of evaluating security and reliability.

EMR-Link is provided as an ASP model, where orders are transmitted securely to the central EMR-Link system over the Internet, and results are returned over the Internet to the EMR. EMR-Link also has secure electronic links to its lab partners; the details of these communication links vary and are negotiated with each lab.

External Communications Architecture
In order to connect to the EMR, EMR-Link relies on two client-side components which run within the EMR environment:

- The Process Orders Form: this is an encounter form installed within the EMR. It allows the user to initiate various ordering functions, some of which involve communication with the EMR-Link system.

- The EMR-Link Connector: this is an executable which is installed in the EMR client software folder, and which provides a communication link from the EMR to EMR-Link. This connector is required because the Centricity EMR doesn’t have a robust and secure way to send data over the Internet directly. The Connector has no local configuration information or registry settings; it is controlled completely by data sent to it on invocation.

The Connector also serves in a separate role for downloading results. To perform this function, the connector is configured via the Windows Task Scheduler to periodically connect to the EMR-Link system and download results into the DTS inbox. Configuration information for the particular connection is set via environment variables in the results.bat file, which runs the connector.

In addition to communication to EMR-Link initiated from the EMR, EMR-Link has a web application which is used for configuration management, as well as for functions such as reporting and access to order history.

External Security Considerations

Transport and Encryption
All communications from the EMR-Link Connector to the EMR-Link servers, and all operations within the web application, are done over HTTPS. All communications are initiated from the client environment [EMR or web browser] so no inbound connections to the client environment are required.

Authentication
For operations initiated from the EMR, EMR-Link assumes that the EMR provides user-level authentication. Thus the user doesn’t need to log in separately to EMR-Link when...
sending an order. The client EMR is identified and authenticated using an authorization code created when the client account is set up in EMR-Link.

This authorization code is also used to identify and authenticate the Connector when it connects to download results.

When the web application is being used separately from the EMR, users log into the web application using a user name and password. Each user login is configured with a set of access rights, so that only authorized users have access to confidential patient information.

**Communication Link to the Lab**

The details of lab communications vary depending on the needs of the particular lab. A typical arrangement is for the EMR-Link Interface Engine to communicate with the lab’s Interface Engine using sockets over VPN. However, some labs use proprietary methods.

Orders are sent to the lab in HL7 format; details of the HL7 format are tailored to the needs of the particular lab. Typically the lab identifies the EMR-Link client by an account number or site ID embedded in the message.

When results are returned from the lab, an account number in the result message identifies the EMR-Link client. EMR-Link performs additional edits to the result data to ensure that it can be imported successfully by the EMR, and will be formatted in a reasonable way. Details of these edits are negotiated with each lab.

**Internal Architecture and Security**

The EMR-Link system currently consists of three servers, housed at the ServerBeach data center in Virginia. Additional servers will be added as performance requirements dictate. The server roles are:

- **Web server** – this server provides the EMR-Link web services and web application, as well as hosting the Ignis Systems Corporation public website.
- **Database server** – this server houses the databases used by EMR-Link.
- **VPN gateway** – this server provides the termination point for all partner VPN’s. ServerBeach doesn’t provide for customer-specific hardware [such as a Cisco firewall], so EMR-Link uses a software-based VPN system [Linux/OpenSwan].

Servers are configured with a minimum number of user accounts, and run only the required services. Windows Firewall is configured on each server. The database server is configured to only accept connections from the web server’s IP address, and operates on a non-default port. Communication between the VPN gateway and the web server is over an internal VPN.

**Data Management and Reliability**

The EMR-Link primary database is backed up nightly, and nightly backups are retained for at least 30 days. In addition there is a monthly backup which is retained for six months.

Order which have already been transmitted to the lab, and results which have already been downloaded to the EMR, are retained for 180 days.
EMR-Link uses several secondary databases containing compendium data provided by the labs. These databases are not backed up but the source data can be reloaded automatically if required.

**Software Practices**

All EMR-Link software is managed through the SVN Configuration management system. A separate testing environment is maintained to validate software changes prior to the software being deployed to the production environment.

The EMR-Link system is designed to allow client accounts to be in either a “test” or “live” mode. Each lab generally has a communication link for test orders/results and a separate link for live orders/results. A client account in test mode will only send orders through the lab’s test connection, and similarly for live mode. When results are received they are tagged as test or live results depending on whether they were received by the test or live link from the lab. These are then selectively downloaded to the EMR depending on whether the EMR is requesting test or live results.