

# EHR TECHNOLOGY & HOSTING

There are two primary factors that affect how secure your EHR is and how well your EHR system runs:

- 1) The Underlying Technology Design
- 2) How and Where the System Application and Data Are Stored

## TECHNOLOGY

EHRs are designed to be client-server, browser-based or Internet-based:

### **Client-Server:**

Client-server is a term for computer systems where the customer's PCs/devices communicate directly with one or more servers that only house only that customer's data and usually are located on the customer's premises. Most EHRs designed prior to the year 2000 are client-server design.

### **Browser-Based:**

A browser-based system was designed for access through a login on a public web site with all applications and data hosted remotely. In this model the user must use a browser such as Internet Explorer or Chrome and no portion of the application resides on the user's computer.

### **Internet-Based:**

An Internet-based system was designed for access through a login on directly from the user's computer with a piece of the application on the user's computer and the majority of the application/program and all of the data hosted remotely. In this model the user does not use a browser and the portion of the application residing on the user's computer is used, in part, to connect to the remotely hosted application and data.

## WHERE AND HOW DATA IS STORED

This is vitally important to data accessibility and security. Options include:

### Locally/Client Hosting:

With a local/client hosted model the applications (programs) and all data are located on servers hosted on the customer's premises. This model relies on the customer to perform server maintenance, including operating system upgrades. Data is stored onsite but may also be backed up by the vendor off-site or the customer may be required to perform regular back-ups.


### Public Cloud Hosting:

A portion of the applications and/or data are hosted in a remote data center run by a public cloud hosting service such as Amazon, Google or Microsoft Azure. In the public cloud the same servers are typically used to host data from multiple disparate companies in separate partitions.

### Dedicated Hosting:

A portion of the applications and/or data are hosted remotely by the vendor in a data center on servers owned by the vendor and only used for that vendor's customers. Banks use Dedicated Hosting for their customer's data and access via remote banking apps.

## THE POSSIBLE CONFIGURATIONS

	CLIENT-SERVER	BROWSER-BASED	INTERNET-BASED
<b>DEDICATED HOSTING</b>	Some vendors may call this "Private Cloud". Vendor must maintain separate servers for each customer – may not be upgraded or maintained timely. System response time may be very slow as system was not designed for remote hosting	Gateway to the application via a public website may diminish security. Requires use of specific browsers. May be slow on lower band Internet connections because of volume of data going through the Internet.	The app is loaded one time on the local device enabling access/login - does not use browser or login from public website. Fast response times even over low band-width Internet connections because fixed portions of the app are on the user's device. 
<b>PUBLIC CLOUD</b>	Same as above plus additional potential data exposure via the public cloud	Same as above plus additional potential data exposure via the public cloud	Potential data exposure via the public cloud
<b>LOCALLY HOSTED</b>	Customer must maintain and upgrade servers, operating systems, etc. Security not as strong as vendor hosting.	N/A	N/A



## HOW CAN A CUSTOMER FIND OUT THIS INFORMATION?

### **Client-Server:**

If the vendor offers the option of hosting your own system, even if they offer remote hosting, more than likely the basic design/technology is client-server. If the vendor offers both local and remote hosting ask them how the systems differ.

### **Public Cloud:**

Ask the vendor who owns the servers where the application and data are stored. If any company other than the vendor owns the servers it is a public cloud.

### **Dedicated Hosting:**

Ask the vendor the name, location and security level (tier) of the data center where the applications and data are stored. Ask the vendor where and how the data is backed up to a secondary data center.

***If a vendor will not or cannot answer the above questions ask yourself if you want to trust your patient data to that vendor.***

## SEVOCITY - A SECURE, SCALABLE, DEDICATED HOSTED MODEL

Sevocity was designed for the Internet. Every piece of our hardware and software was explicitly designed for our system and are under our control. With Sevocity:

- There is a small portion of the application on your device that houses colors, screen designs and information that does not change. This allows only true core data to have to be shared over the Internet, making the system extremely fast and responsive. It also means that you can even use Sevocity over slow Internet speeds such as mobile hot spots.
- Your data is stored in a true data center on servers we own and back-up to a separate datacenter at our headquarters.
- The Sevocity application (the program) is stored on servers with constant load balancing and diagnostics. All customers use the program from these servers. This ensures that the system never comes close to capacity and all customers have the current version and receive automatic system updates.
- All patient data is stored encrypted when at rest, even within our database(s). Furthermore each patient record is encrypted with the Clinic's unique secret key so that only authorized clinic users may decrypt the patent data.

Our commitment to you and your patients is to keep your data secure at all times.

