13. POCT CONNECTIVITY GLOSSARY

ADT: An admission, discharge, and transfer (ADT) system is a backbone system for the structure of other types of business systems. Using the ADT system, patient information can be shared, when appropriate, with other health care facilities and systems (McGonigle, D., & Mastrain, K., 2012).

DHCP: Stands for "Dynamic Host Configuration Protocol." DHCP is a protocol that automatically assigns a unique IP address to each device that connects to a network. With DHCP, there is no need to manually assign IP addresses to new devices. Therefore, no user configuration is necessary to connect to a DCHP-based network. Because of its ease of use and widespread support, DHCP is the default protocol used by most routers and networking equipment.

Docking stations: Docking stations may also refer to hardware used to connect tablets, smartphones, and other portable devices to one or more peripherals. However, these devices are generally called "docks" and typically have fewer I/O connections than a laptop dock.

FTP: "File Transfer Protocol." FTP is a protocol designed for transferring files over the Internet. Files stored on an FTP server can be accessed using an FTP client, such as a web browser, FTP software program, or a command line interface.

Hardwired Computers: Built into a computer's hardware and thus not readily changed. (Of a terminal) connected to a computer by a direct circuit rather than through a switching network. (Of electrical or electronic components) connected by hardwiring.

HTTP: "Hypertext Transfer Protocol." HTTP is the protocol used to transfer data over the web. It is part of the Internet protocol suite and defines commands and services used for transmitting webpage data.

HTTPS: "HyperText Transport Protocol Secure." HTTPS is the same thing as HTTP but uses a secure socket layer (SSL) for security purposes. Some examples of sites that use HTTPS include banking and investment websites, e-commerce websites, and most websites that require you to log in.

Interface: A common boundary or interconnection between systems, equipment, concepts, or human beings. Computer hardware or software designed to communicate information between hardware devices, between software programs, between devices and programs, or between a device and a user.

Lantronix: Lantronix Device Servers enable M2M communications either between the computer and serial device, or from one serial device to another over the Internet or Ethernet network using "serial tunneling."

Middleware: Middleware has two separate but related meanings. One is software that enables two separate programs to interact with each other. Another is a software layer inside a single application that allows different aspects of the program to work together. The most common type of middleware is software that enables two separate programs to communicate and share data. An example is software on a Web server that enables the HTTP server to interact with scripting engines like PHP or ASP when processing webpage data. Middleware also enables the Web server to access data from a database when loading content for a webpage. In each of these instances, the middleware runs quietly in the background, but serves as an important "glue" between the server applications. Middleware also helps different applications communicate over a computer network. It enables different protocols to work together by translating the information that is passed from one system to another. This type of middleware may be installed as a "Services-Oriented Architecture" (SOA) component on each system on the network. When data is sent between these systems, it is first processed by the middleware component, then output in a standard format that each system can understand.

Remote Access: The ability to access your computer from a remote location. Programs like PC Anywhere (Windows), Remote Access (Mac), and Timbuktu (Windows and Mac) allow users to control remote computers from their local machine. In order for a remote access connection to take place, the local machine must have the remote client software installed and the remote machine must have the remote server software installed. Also, a username and password are almost always required to authenticate the connecting user.

Remote Desktop: Remote desktop technology makes it possible to view another computer's desktop on your computer. This means you can open folders, move files, and even run programs on the remote computer, right from your own desktop. Both Windows and Macintosh computer support remote desktop connections, though they use different implementations.

Servers: A server is a computer that provides data to other computers. It may serve data to systems on a local area network (LAN) or a wide area network (WAN) over the Internet.

SQL: "Structured Query Language," and can be pronounced as either "sequel" or "S-Q-L." It is a query language used for accessing and modifying information in a database.

SSL: "Secure Sockets Layer." SSL is a secure protocol developed for sending information securely over the Internet. Many websites use SSL for secure areas of their sites, such as user account pages and online checkout. Usually, when you are asked to "log in" on a website, the resulting page is secured by SSL.

Virtual: Virtual machines provide similar functionality to physical machines, but they do not run directly on the hardware. Instead, a software layer exists between the hardware and the virtual machine. The software that manages one or more VMs is called a "hypervisor" and the VMs are called "guests" or virtualized instances. Each guest can interact with the hardware, but the hypervisor controls them. The hypervisor can start up and shut down virtual machines and also allocate a specific amount of system resources to each one.

VPN: A "virtual private network" allows the extension of a private network across a public network in a secure, potentially protected manner.

Wi-Fi: Wi-Fi is a wireless networking technology that allows computers and other devices to communicate over a wireless signal. It describes network components that are based on one of the 802.11 standards developed by the IEEE and adopted by the Wi-Fi Alliance. Examples of Wi-Fi standards, in chronological order, include: 802.11a; 802.11b; 802.11g; 802.11n; 802.11ac. Wi-Fi is the standard way computers connect to wireless networks. Nearly all modern computers have built-in Wi-Fi chips that allows users to find and connect to wireless routers. Most mobile devices, video game systems, and other standalone devices also support Wi-Fi, enabling them to connect to wireless networks as well. When a device establishes a Wi-Fi connection with a router, it can communicate with the router and other devices on the network. However, the router must be connected to the Internet (via a DSL or cable modem) in order to provide Internet access to connected devices.

Wireless: Any system or device, as cell phone, for transmitting messages or signals by electromagnetic waves.