PARCA Exam Entry Requirements

This document contains the detailed entry requirements for the entry requirements for taking the exam that is needed as a pre-requisite for the PARCA CPIA and CPSA certifications. The focus is on either general technical understanding or general clinical understanding.

A. Technical entry requirements (prerequisites for people with clinical background):

1. Computer basics:

1.1 Hardware: A computer has hardware components, i.e. CPU, memory, Disk, removable media, display card and display and data entry devices such as keyboard and mouse. There are several standard interfaces, such as RS232, USB, and network and dedicated modem interfaces. – Know how to distinguish these devices and function of each of them.

1.2 Software: Software can be divided into operating system, drivers to deal with specific hardware features, utilities such as database and word processing and application software. Know how to distinguish these and their function.

1.3 CPU: The CPU determines to a high degree the performance of the computer. – Know impact of processor speed and I/O path width (in bits) as well as impact of dedicated processing boards.

1.4 Memory: Memory determines performance, both memory speed and capacity. – Know impact of memory parameters.

1.5 Disk technology: Disk performance is typically determined by type and access (I/O channel, or network). Other parameters are speed, reliability, redundancy, impact of formatting and capacity. Know impact of disk parameters on performance.

1.6 IP / MAC Addresses: Computers communicate via networks, which means that there is an addressing scheme needed so others can access them. – Know function of IP and MAC address and how to manage these.

1.7 Exchange media: Exchange media are DVD, CD, removable memory sticks, etc. – Know how to address these media on a computer and to distinguish between Read-Only and Read/Write functionality.

2. Operating system basics

2.1 Unix: Unix, or derivatives (LINUX) is often used for high availability computers such as servers. – Know basic UNIX prompts.

2.2 Windows: Windows is a common operating system used for desktop computers. – Know basic windows concepts, such as directory structures, windows task manager and control panel features and how to change basic settings.

2.3 DOS prompts: DOS prompts are often used for basic hardware and low level features. – Know how to get to the DOS prompt and to execute basic commands.

3. Database basics

3.1 Hierarchical, relational, object databases: Databases provide the capability for storing and retrieving information. – Know the difference between, and characteristics of different database types.

3.2 Basic SQL knowledge: The ANSI SQL language is the most common used for database access and allows for direct access for troubleshooting, maintenance, and special reporting. – Know basic SQL commands to access data from a relational database.

4. Data representations:

4.1 Binary data format: Information is stored in computer memory as zero's and ones, i.e. in a binary format. For numbers, each position in a data field can represent a power of two. – Convert a binary representation to a numeric value.

4.2 Bits, bytes: Each zero/one in a data field is called a "bit" multiple of 8 bits are called Bytes. – Know actual number of bits represented by KB, MB, GB, TB.

4.3 Hexadecimal: Information can be represented as groups of bits (e.g. 3 bits is octal, 4 is hexadecimal).- Know how to interpret a hexadecimal number.

4.4 Signed/unsigned data: The high bit of a data filed can be used to indicate a negative number. – Know how to convert a signed data filed back to a numeric value.

4.5 Floating point: Non-integer values can be represented with a separate exponent. – Know how to interpret a floating point value.

4.6 Monochrome, RGB: A data field could represent a certain grayscale value (Black/White) or a value in a color mapping (for example, Red/Green/Blue). Other color mappings are possible as well (YBR, etc.). – Know how to interpret grayscale and color values.

5. Networking technology:

5.1 WAN/LAN, T1, ISDN, DSL: Network technology is used to either acces a local or wide area network or access the network using an access path such as a high speed T1 line, ISDN or using DSL technology. – Know different terminology and technologies for networks and access connections.

5.2 Internet (http, url, domains): Internet access is commonly used for e-mail and to exchange information with user internet users. – Know function of domains and how to identify them with a url as well as function of www and http. Know function of RFC's and structure of Internet governance.

5.3 ISO model: A network connection can be thought of using different per-to-peer layers using their own protocols. – Know function and features of each 7 layers of the ISO model.

5.4 Ethernet, TCP/IP: Most network connections use the TCP/IP for layer 4 and Etheret for layer 2 communication. – Know principles of each protocol, i.e. addressing and protocol type.

5.5 Packet switching, circuit switching: Most commonly used public networks use either packet or circuit switching technology. – Know the characteristics of each of these protocols.

5.6 Throughput, bandwidth, level of service parameters: Network access is determined by several critical parameters used for planning and forecasting the required network topology. – Know meaning and how to characterize these parameters

6. Basic Security Concepts:

6.1 System security in general: Security is typically characterized as authentication, authorization, confidentiality and integrity. – Know how to characterize and identify each of the security components.

6.2 Authentication: First item typically done when accessing data is authenticating of entity that is doing the access. – Know of authentication methods including certificates.

6.3 Authorization: Authorization is typically done at application level based on certain roles. – Know authorization functionality and how it fits in the overall security scheme.

6.4 Confidentiality: Confidentiality is mostly implemented using encryption. – know strengths of different algorithms and impact of key length as well as symmetric-asymmetric and public/private key function.

6.5 Integrity: data integrity can be implemented with digital signatures, checksums, etc. – Know how digital signatures work, function of hashing and keys.

B. Clinical entry requirements (pre-requisites for people with technical background):

1. Basic medical terminology: The medical profession uses certain terms that appear in orders, such as in the diagnosis or pre-condition. – Be familiar with the most common medical terms.

2. Basic human anatomy: Imaging is typically done of certain body parts and/or organs. – Know the general skeletal system & major organs so that images can be related back to the patient body parts.

3. Radiology Imaging basics:

3.1 Principles of different modalities (CR, DR, XR, XA, RF, US, MR, NM, CT): Each modality has different characteristics based on how the images are generated, i.e. using X-ray, electro-magnetic energy, radiation, etc. - Need to know the principle of how the energy is captured and imaged including typical exam types and applications.

3.2 Basic operational procedural knowledge of computer radiology equipment: Each exam requires different handling and operation by a technologist, and has a specific length and characteristics. – Need to know typical examination procedures and technologist handling.

3.3 Image characteristics for each modality: Each image has specific characteristics regarding noise, resolution, size of image and relationship with others (CINE loops, functional imaging). – Recognize typical image parameters for each modality.

3.4 Positioning and viewing techniques and terminology: A patient is positioned in a certain way (e.g. L/R; PA/LAT) with regard to the imaging equipment. Images are identified as such. – Know most important viewing and positioning techniques.

3.5 QA / QC: Quality control and assurance are critical in an imaging department to make sure the appropriate technique is used for optimal image quality while trading off potential harm to the patient. – Know where and what a typical QA program consist of and what parameters are typically impact the image quality.

3.6 Collimation versus shuttering: Proper collimation is critical to achieve optimal image quality. – Know about the use of shutters, grids, and the impact it might have on images.

4. Typical process flow (“Completing the exam cycle”)

4.1 Physician order: Orders should contain all pertinent information to perform an imaging procedure. – Know what typical orders information consist of, and what is critical for certain procedures (e.g. allergy, pregnancy status, lab values, weight, history)

4.2 Performance of exam: Exams are sometimes scheduled, depending on the procedure or urgency. Each exam type has a different series of steps to perform. – Know a typical workflow for each modality.

4.3 Results reporting (dictation & speech recognition): The technologist does a “hands-off” to a physician who performs a diagnosis using a dictation system or speech

recognition. – Know the workflow for the radiologist using a worklist, potentially sharing this list with peers, till the report is signed off and approved.

4.4 Remote system access for image viewing: In some cases, the images with the requisition are sent to a remote location, e.g. for reading images at night. – Know the specific workflow to get a preliminary read from a physician from a remote location.

5. How to handle prior exams & outside exams:

5.1 Film & digitization: Prior exams might have to be fetched, either as film or, if digital, potentially from an off-line media. In some cases, the images might have to be digitized. – Know the digitization workflow, including potential issues with conflicting identifiers in the case the films are brought in from another institution.

5.2 Import CD's: Increasingly, patients are bringing their images on CD's that have to be imported and/or accessed by the physician making the diagnosis. – Know the appropriate workflow and identify common issues with importing CD's such as the availability of proprietary data, embedded viewers, and identifiers that could give potential conflicts.