SUBTLE MEDICAL

DICOM Conformance Statement

Conformance Statement Overview

The Subtle Medical product ecosystem implements the necessary DICOM services to anonymize, transfer, store, process, and return DICOM images from customer workstations, file systems, and storage devices. Table 1 lists the network services supported by Subtle Medical products. Table 2 lists and describes Subtle Medical products. There is no support for Media Storage Application Profiles because processed images are returned and stored on a customer's device.

Table 1: Subtle Medical Networking Related Services

SOP Class	User of Service (SCU)	Provider of Service (SCP)
CT Image Storage	Yes	Yes
MR Image Storage	Yes	Yes
Nuclear Medicine Image Storage	Yes	Yes
Positron Emission Tomography Image Storage	Yes	Yes

Table 2: Subtle Medical Products That Implement DICOM Services

Product Name	Description
SubtlePET™	A SaMD using an AI/ML model that enhances MRI images.
SubtleMR™	A SaMD using an AI/ML model that enhances PET images (including PET/CT and PET/MRI).
SubtleEDGE™	An MDDS for interfacing between SubtleApps (i.e., SubtleMR, SubtlePET) and DICOM-capable medical devices.
SubtleCLOUD™	Backend SaMD that enables image storage and SubtleApps to process medical images in the cloud.
SubtleSHARE™	Software component to share de-identified DICOM images with Subtle via SubtleCLOUD.
Subtle Console	A website used to view the usage, configuration, and performance of SubtleApps as well as view permitted images stored in SubtleCLOUD.

Note: Refer to the product's User Manual for the indications for use, safety info, and operating procedures.

Manufacturer Information

Subtle Medical, Inc
883 Santa Cruz Ave, Suite 205
Menlo Park, CA, 94025
United States of America

Contact

Help Center: Customer Operations Help Center
Email: support@subtlemedical.com
Phone: 1-650-397-8709

Table of Contents

Introduction

Audience

This document is for Subtle Medical customers to help understand how Subtle Medical AI/ML imaging applications (i.e., SubtlePET™ and SubtleMR™) and SubtleEDGE™ (with SubtleCLOUD™ for cloud execution) will integrate into their healthcare facility. Customer representatives include both those responsible for overall imaging network policy and architecture, as well as integrators who need to have a detailed understanding of the DICOM features of the product. This document contains some basic DICOM definitions so that any reader may understand how this product implements DICOM features. However, integrators should understand all the DICOM terminology, how the tables in this document relate to the product's functionality, and how that functionality integrates with other devices that support compatible DICOM features.

Remarks

The scope of this DICOM Conformance Statement is to facilitate integration between Subtle Medical products and other DICOM products. The Conformance Statement should be read and understood in conjunction with the DICOM Standard. DICOM by itself does not guarantee interoperability. The Conformance Statement does, however, facilitate a first-level comparison for interoperability between different applications supporting compatible DICOM functionality.

This Conformance Statement is not supposed to replace validation with other DICOM equipment to ensure proper exchange of intended information. Please be aware of the following important issues:

- The comparison of different Conformance Statements is just the first step towards assessing interconnectivity and interoperability between the product and other DICOM conformance equipment.
- Test procedures should be defined and executed to validate the required level of interoperability with specific compatible DICOM equipment, as established by the healthcare facility.

References

- DICOM Library, DICOM Tags https://www.dicomlibrary.com/dicom/dicom-tags/
- NEMA PS3 DICOM Standard, http://medical.nema.org/
- NEMA Value Representation, https://dicom.nema.org/dicom/2013/output/chtml/part05/sect_6.2.html
- LBL012 SubtleEDGE User Manual
- LBL055 SubtleEdge On-Prem Installation Requirements and Recommendations
- LBL056 SubtleEdge Cloud Installation Requirements and Recommendations

Note: All documents with the LBL prefix are Subtle Medical instructions and other information about Subtle Medical products, which are available from your CSM.

Abbreviations

- AE Application Entity

- AET Application Entity Title
- AI/ML Artificial Intelligence/Machine Learning
- AWS Amazon Web Services
- CT Computed Tomography
- CSM Customer Success Manager
- DCS DICOM Conformity Statement
- DICOM Digital Imaging and Communications in Medicine
- HTTPS Hypertext Transfer Protocol Secure
- ISO International Organization for Standards
- IT Information Technology
- JPEG Joint Photographic Experts Group
- LO Long String
- LT Long Text
- MDDS Medical Device Data Systems
- MRI Magnetic Resonance Imaging
- MQTT Message Queuing Telemetry Transport
- PACS Picture Archiving And Communication System
- PDU Protocol Data Unit
- PET Positron Emission Tomography
- PHI Protected Health Information
- SaMD Software as a Medical Device
- SCP Service Class Provider
- SCU Service Class User
- SOP Service Object Pair
- UID Unique Identifier
- VR Value Representation

Terms and Definitions

Informal definitions are provided for the following terms used in this Conformance Statement. The DICOM Standard is the authoritative source for formal definitions of these terms.

- **Abstract Syntax** – the information agreed to be exchanged between applications, generally equivalent to a Service/Object Pair (SOP) Class. Examples : Verification SOP Class, Modality Worklist Information Model Find SOP Class, Computed Radiography Image Storage SOP Class.

- **Application Entity (AE)** – an end point of a DICOM information exchange, including the DICOM network or media interface software; i.e., the software that sends or receives DICOM information objects or messages. A single device may have multiple Application Entities.

- **Application Entity Title** – the externally known name of an *Application Entity*, used to identify a DICOM application to other DICOM applications on the network.

- **Application Context** – the specification of the type of communication used between *Application Entities*. Example: DICOM network protocol.

- **Association** – a network communication channel set up between *Application Entities*.

- **Attribute** – a unit of information in an object definition; a data element identified by a tag. The information may be a complex data structure (Sequence), itself composed of lower level data

elements. Examples: Patient ID (0010,0020), Accession Number (0008,0050), Photometric Interpretation (0028,0004), Procedure Code Sequence (0008,1032).

- **Information Object Definition (IOD)** – the specified set of *Attributes* that comprise a type of data object; does not represent a specific instance of the data object, but rather a class of similar data objects that have the same properties. The *Attributes* may be specified as Mandatory (Type 1), Required but possibly unknown (Type 2), or Optional (Type 3), and there may be conditions associated with the use of an Attribute (Types 1C and 2C). Examples: MR Image IOD, CT Image IOD, Print Job IOD.

- **Joint Photographic Experts Group (JPEG)** – a set of standardized image compression techniques, available for use by DICOM applications.

- **Media Application Profile** – the specification of DICOM information objects and encoding exchanged on removable media (e.g., CDs)

- **Module** – a set of *Attributes within an Information Object Definition* that are logically related to each other. Example: Patient Module includes Patient Name, Patient ID, Patient Birth Date, and Patient Sex.

- **Negotiation** – first phase of Association establishment that allows *Application Entities* to agree on the types of data to be exchanged and how that data will be encoded.

- **Presentation Context** – the set of DICOM network services used over an *Association*, as negotiated between *Application Entities*; includes *Abstract Syntaxes* and *Transfer Syntaxes*.

- **Protocol Data Unit (PDU)** – a packet (piece) of a DICOM message sent across the network. Devices must specify the maximum size packet they can receive for DICOM messages.

- **Security Profile** – a set of mechanisms, such as encryption, user authentication, or digital signatures, used by an *Application Entity* to ensure confidentiality, integrity, and/or availability of exchanged DICOM data.

- **Service Class Provider (SCP)** – role of an *Application Entity* that provides a DICOM network service; typically, a server that performs operations requested by another Application Entity (Service Class User). Examples: Picture Archiving and Communication System (image storage SCP, and image query/retrieve SCP), Radiology Information System (modality worklist SCP).

- **Service Class User (SCU)** – role of an Application Entity that uses a DICOM network service; typically, a client. Examples: imaging modality (image storage SCU, and modality worklist SCU), imaging workstation (image query/retrieve SCU).

- **Service/Object Pair (SOP)** Class – the specification of the network or media transfer (service) of a particular type of data (object); the fundamental unit of DICOM interoperability specification. Examples: Ultrasound Image Storage Service, Basic Grayscale Print Management.

- **Service/Object Pair (SOP) Instance** – an information object; a specific occurrence of information exchanged in a *SOP Class*. Examples: a specific x-ray image.

- **Tag** – a 32-bit identifier for a data element, represented as a pair of four digit hexadecimal numbers, the "group" and the "element". If the "group" number is odd, the tag is for a private (manufacturer-specific) data element. Examples: (0010,0020) [Patient ID], (07FE,0010) [Pixel Data], (0019,0210) [private data element].

- **Transfer Syntax** – the encoding used for exchange of DICOM information objects and messages. Examples: *JPEG* compressed (images), little endian explicit value representation.

- **Unique Identifier (UID)** – a globally unique "dotted decimal" string that identifies a specific object or a class of objects; an ISO-8824 Object Identifier. Examples: Study Instance UID, SOP Class UID, SOP Instance UID. V

- **Value Representation (VR)** – the format type of an individual DICOM data element, such as text, an integer, a person's name, or a code. DICOM information objects can be transmitted with either explicit identification of the type of each data element (Explicit VR), or without explicit identification (Implicit VR); with Implicit VR, the receiving application must use a DICOM data dictionary to look up the format of each data element.

Basics of DICOM Communication

This section describes terminology used in this Conformance Statement for the non-specialist. The key terms used in the Conformance Statement are highlighted in *italics* below. This section is not a substitute for training about DICOM, and it makes many simplifications about the meanings of DICOM terms.

Two Application Entities (devices) that want to communicate with each other over a network using DICOM protocol must first agree on several things during an initial network "handshake". One of the two devices must initiate an *Association* (a connection to the other device), and ask if specific services, information, and encoding can be supported by the other device (*Negotiation*).

DICOM specifies a number of network services and types of information objects, each of which is called an *Abstract Syntax* for the Negotiation. DICOM also specifies a variety of methods for encoding data, denoted *Transfer Syntaxes*. The Negotiation allows the initiating Application Entity to propose combinations of Abstract Syntax and Transfer Syntax to be used on the Association; these combinations are called *Presentation Contexts*. The receiving Application Entity accepts the Presentation Contexts it supports.

For each Presentation Context, the Association Negotiation also allows the devices to agree on Roles – which one is the *Service Class User* (SCU - client) and which is the *Service Class Provider* (SCP - server). Normally the device initiating the connection is the SCU, i.e., the client system calls the server, but not always.

The Association Negotiation finally enables exchange of maximum network packet (PDU) size, security information, and network service options (called *Extended Negotiation* information).

The Application Entities, having negotiated the Association parameters, may now commence exchanging data. Common data exchanges include queries for worklists and lists of stored images, transfer of image objects and analyses (structured reports), and sending images to film printers. Each exchangeable unit of data is formatted by the sender in accordance with the appropriate *Information Object Definition*, and sent using the negotiated Transfer Syntax. There is a Default Transfer Syntax that all systems must accept, but it may not be the most efficient for some use cases. Each transfer is explicitly acknowledged by the receiver with a *Response Status* indicating success, failure, or that query or retrieve operations are still in process.

Two Application Entities may also communicate with each other by exchanging media (such as a CDR). Since there is no Association Negotiation possible, they both use a *Media Application Profile* that specifies "pre-negotiated" exchange media format, Abstract Syntax, and Transfer Syntax.

Service Workflow

On-Premise Execution Workflow

For on-premise execution mode, there is both an online and offline option in terms of how your SubtleEDGE server interacts with the Subtle Platform. In both cases, the DICOM images are processed within your local environment on your own hardware, the main difference between the two is the level of visibility and capabilities available to Subtle Medical employees to support your deployment. We encourage customers to deploy in online mode, simply because it helps us more quickly assess and address any issues you have with the solution.

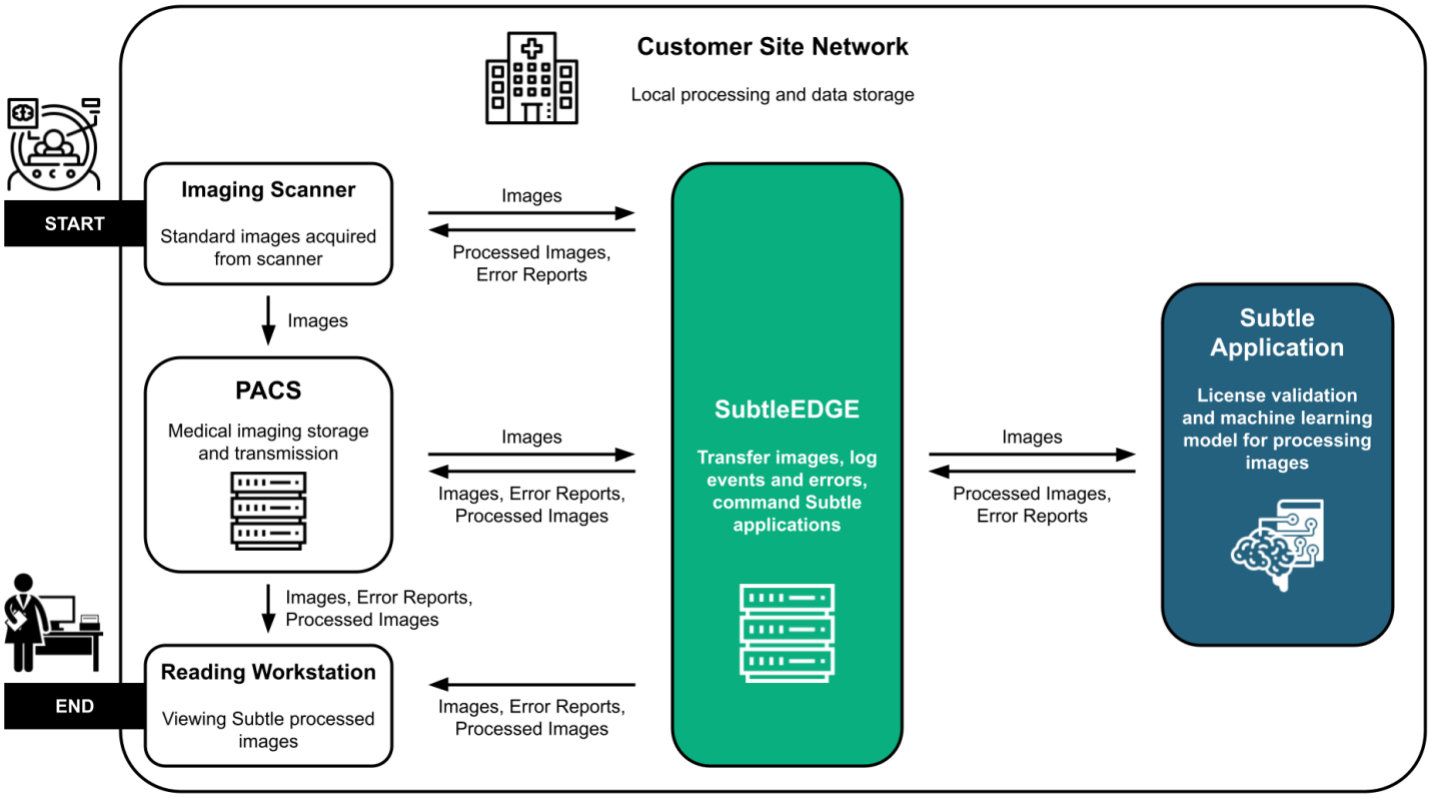

Figure 1: Subtle Medical On-Premise Execution Offline Workflow

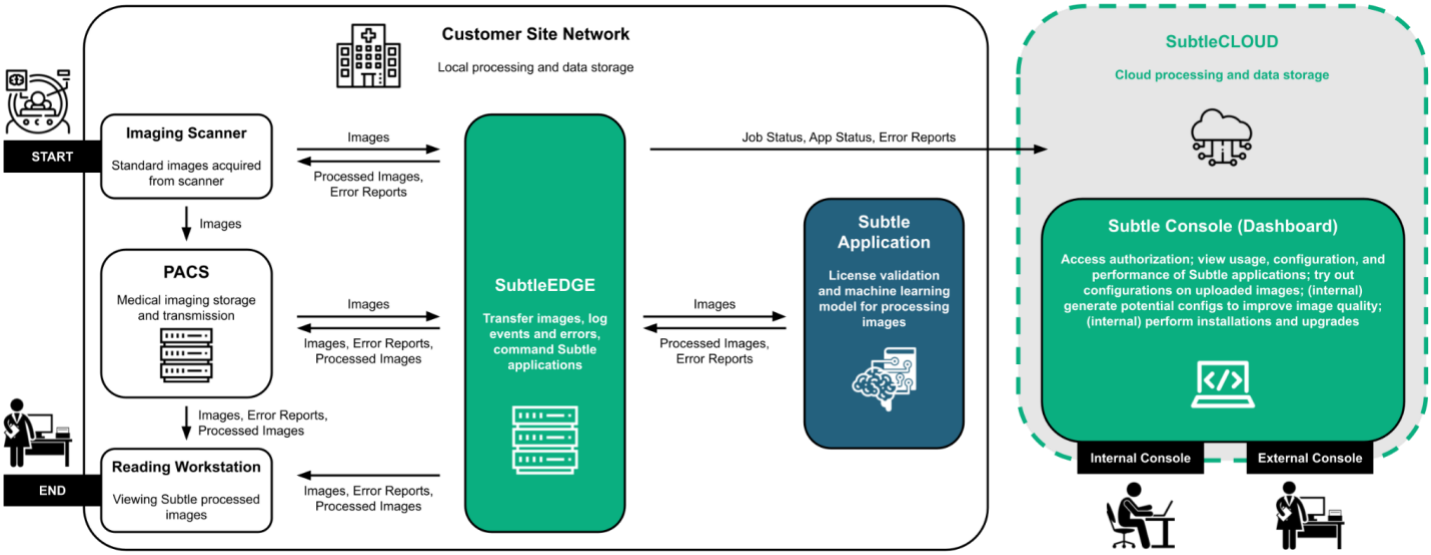

Figure 2: Subtle Medical On-Premise Execution Online Workflow

Cloud Execution Workflow

For cloud execution mode, Subtle image processing applications are executed on the SubtleCLOUD, a secure and resilient application environment that enables better scalability. It also requires much less computing requirements on the on-premise gateway host device. PHI and other identifiers are removed from the DICOM images by SubtleEDGE before being sent to the cloud, but even so Subtle treats this environment as if it were storing ePHI: All the data is encrypted at rest and during transfer, we have a BAA in place with AWS, and we have a information security program in place. The environment undergoes a variety of internal and external audit activities each year, including an annual SOC 2 + HIPAA audit.

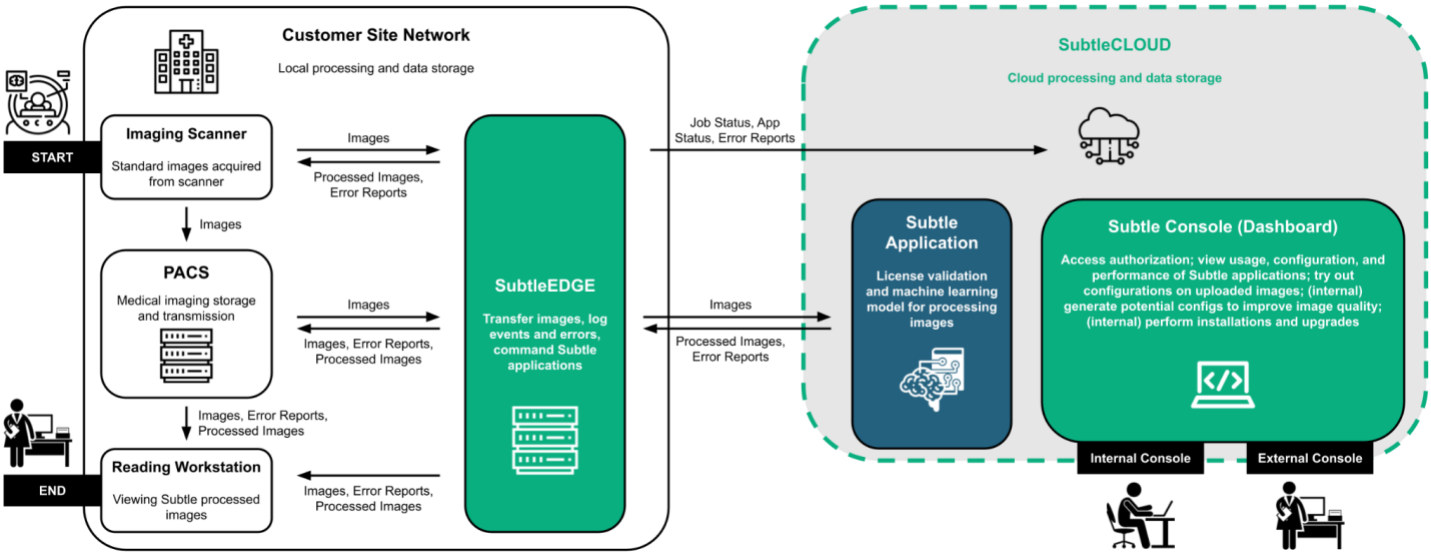

Figure 3: Subtle Medical Cloud Execution Workflow

SubtleShare

SubtleShare is a program where customers share de-identified DICOM images with Subtle via SubtleCLOUD. Sharing of these images takes place after processing on a per study basis. For on-premise deployments, the deployment must be an online deployment for sharing to take place. This program is part of the contract unless you opt out, so please check with the business owner of this application and your Subtle Medical CSM to determine whether this feature will be enabled so that you can factor in any additional bandwidth requirements for your deployment plan.

Removal of PHI for Cloud Processing

For customers who are utilizing cloud processing, PHI data is removed from the DICOM images prior to any job leaving the customer's network. The SubtleEDGE application generates a unique JobID for each received image data set, and the DICOM tags containing PHI are replaced with null values while the original PHI values are cached in the local server's memory. The de-identified data with the unique JobID is then sent to the Subtle cloud for processing. Once complete, the processed images are sent from the cloud back to the SubtleEDGE server where the images are re-identified using the cached values prior to being routed to the relevant image worklist/reading location. Once this workflow is completed, all input and output data related to that job (including all PHI) are removed from the SubtleEDGE server as well. The de-identification process is the same for images shared with Subtle via SubtleShare, except the original PHI will not be retained on SubtleEDGE since it won't be re-identified.

Networking

Implementation Model

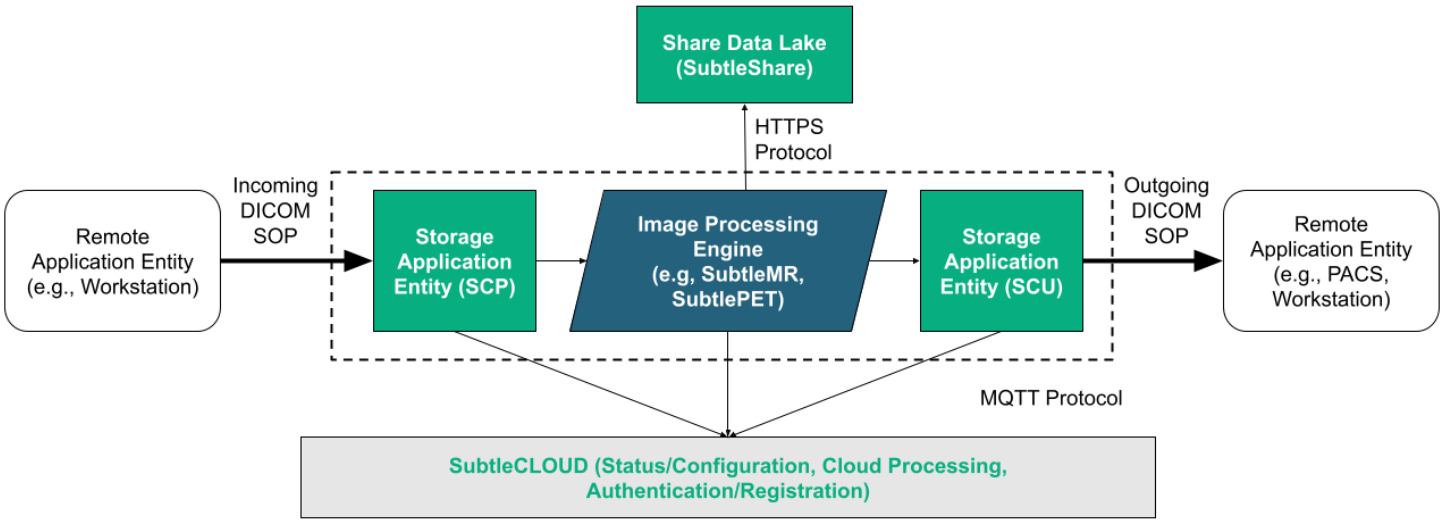

Figure 4: Application Data Flow and Protocols

The Remote Application Entity sends images to the SCP. The SCP sends images to the image processing image engine, which runs a Subtle Medical image processing application such as SubtleMR and SubtlePET. The SCU receives the enhanced images and sends it to a configured Remote Application Entity. Processing and storage, if performed in the cloud, is sent to SubtleCLOUD. Any images that are given permission to share with Subtle Medical will be sent and stored in Subtle Medical's internal data lake.

Functional Definition of AE's

The upstream source for the DICOM initiates an association with the incoming storage AE (SCP). An association request is sent to the destination AE and upon successful negotiation of a Presentation Context the image transfer is started. If the association cannot be opened, the related send-job is set to an error state and can be restarted by the user via the job control interface. By default, the outgoing storage AE (SCU) will retry transmission five times with an exponential backoff (the amount of time the system waits after failure before retrying).

Storage Application Entity Specification

SOP Classes

This Application Entity provides Standard Conformance to the following SOP Classes:

Table 3: SOP Classes for AE Storage

SOP Class	SOP Class UID	SCU	SCP
CT Image Storage	1.2.840.10008.5.1.4.1.1.2	Yes	Yes
MR Image Storage	1.2.840.10008.5.1.4.1.1.4	Yes	Yes
Nuclear Medicine Image Storage	1.2.840.10008.5.1.4.1.1.20	Yes	Yes
Positron Emission Tomography Image Storage	1.2.840.10008.5.1.4.1.1.128	Yes	Yes

Association Policies

General

The DICOM standard application context name for DICOM 3.0 is always proposed:

- Application Context Name: 1.2.840.10008.3.1.1.1

Number of Associations

SubtleEDGE initiates one Association at a time for each destination to which a transfer request is being processed in the active job queue list. Multiple jobs may be concurrently transmitted on separate associations. SubtleEDGE may receive simultaneous associations. There is no maximum number of simultaneous associations set. Number of simultaneous associations set is limited by availability of processing resources.

Asynchronous Nature

SubtleEDGE does not support asynchronous communication (multiple outstanding transactions over a single Association). Maximum number of outstanding asynchronous transactions is 1.

Implementation Identifying Information

The DICOM implementation class and version for AE Storage is:

- Implementation Class UID: 1.2.826.0.1.3680043.8.691.0.20
- Implementation Version Name: 3.6

Description and Sequencing of Incoming Activities

The incoming DICOM SOP, as shown in Figure 4, is initiated by the upstream DICOM device, such as a workstation. This creates a DICOM association, wherein the Remote Application Entity SCU and the SubtleEDGE SCP negotiate the presentation context. The supported SOP Classes are given in Table 3 above. The supported transfer syntaxes are given in Table 4 below.

Once the association is established and the presentation context is negotiated, the SCU may send one or more C-STORE or C-ECHO commands to the SubtleEDGE SCP. Files stored via the C-STORE command are grouped into jobs. Each job consists of all the DICOM files for a particular study that were received in that association or in concurrent associations. This job is then passed to the image processing engine via file system operations.

Description and Sequencing of Outgoing Activities

The outgoing DICOM SOP, as shown in Figure 4, is initiated by the image processing engine upon completion of processing each job. The SubtleEDGE SCU initiates the DICOM association with a Remote Application Entity SCP. The supported SOP Classes are given in Table 3 above. The supported transfer syntaxes are given in Table 4 below.

Once the association is established and the presentation context is negotiated, the SubtleEDGE SCU sequentially sends a C-STORE instruction for each DICOM file in the job.

Supported Presentation Contexts

SubtleEDGE is capable of supporting the Presentation Contexts shown in the following table:

Table 4: Proposed Presentation Contexts for AE Storage

Transfer Syntaxes		Role	Extended Negotiation
Lossless JPEG	1.2.840.10008.1.2.4.70	SCU, SCP	None
Lossless JPEG-LS	1.2.840.10008.1.2.4.80	SCU, SCP	None
Lossy JPEG-LS	1.2.840.10008.1.2.4.81	SCU, SCP	None
Implicit VR Little Endian	1.2.840.10008.1.2	SCU, SCP	None
Explicit VR Little Endian	1.2.840.10008.1.2.1	SCU, SCP	None
Explicit VR Big Endian	1.2.840.10008.1.2.2	SCU, SCP	None
RLE Lossless	1.2.840.10008.1.2.5	SCU, SCP	None

SOP Specific Conformance for SOP Classes

All Storage SOP Classes supported by the Storage AE exhibit the same behavior, except where stated, and are described together in this section.

If a SOP Instance is included in the task and a corresponding Presentation Context is not accepted then the Association is aborted using A-P-ABORT and the task is failed. The failure is logged and reported to the user.

Configuration: AE Title/Presentation Address Mapping

SCP Local AE Title

The SubtleEDGE SCP AE title is configurable through the application configuration file.

Table 5: Configuration for SCP Local AE Title

Application Entity	Default AE Title	Default TCP/IP Port
SubtleMR	SubtleMR	18900
SubtlePET	SubtlePET	18900

SCU Local AE Title

The SubtleEDGE SCU AE Title is configurable through the application routing configuration. By default, the SubtleEDGE SCU uses a calling AE Title of "SubtleEDGE". It can be configured to use any other fixed string that is a valid AE Title, or to be derived from any DICOM tag whose VR is "AE" (AE Title).

Table 6: Configuration for SCU Local AE Title

Application Entity	Default AE Title
SubtleEDGE	SubtleEDGE

Remote AE Title/Presentation Address Mapping

The remote Presentation Address, including the called AE Title used by SubtleEDGE SCU, is specified through the application routing configuration.

DICOM Metadata Tag Value Changes

SubtleApps change certain DICOM values as a part of their processing. These changes are made to remain conformant to both the spirit and the letter of the DICOM standard, as well as to work around manufacturer incompatibilities and accurately reflect the state of the data. In addition to changing the actual image data (i.e., Pixel Data), the SubtleApps modify DICOM tags as described below. The DICOM tags modified by SubtleMR are given in Table 7, the DICOM tags modified by SubtlePET are given in Table 8, and the DICOM tags modified by SubtleEDGE to perform anonymization and reidentification are given in Table 9.

Note that if a customer has PHI/PII in tags not listed in Table 9, the customer can contact Subtle Medical to request additional fields to be anonymized prior to being sent to a Subtle application for processing.

Table 7: DICOM Metadata Tags Modified by SubtleMR

DICOM Tag Name	Tag Coordinates	Modification by SubtleMR
Image Type	(0008, 0008)	Changed from “ORIGINAL” to "DERIVED".
Series Number	(0020, 0011)	Offsets the original value by 100.

DICOM Tag Name	Tag Coordinates	Modification by SubtleMR
Series Description	(0008, 103E)	Applies the suffix "SMR". If using the Evaluation Mode, it will apply the prefix “Eval” and the suffix “SMR1”, “SMR2”, or “SMR3”.
Acquisition Matrix	(0018, 1310)	Phase and frequency encodings are updated to reflect the new image.
SOPInstanceUID	(0008, 0018)	Changed to a new unique value in the prefix specified in the app configuration (if any). Otherwise, changed to a new unique value in the Subtle Medical prefix (1.2.826.0.1.3680043.10.221) unless the manufacturer of the original image is Phillips, in which case it is changed to a new unique value in the Phillips prefix (1.3.46.670589).
SeriesInstanceUID	(0020, 000E)	Changed to a new unique value in the prefix specified in the app configuration (if any). Otherwise, changed to a new unique value in the Subtle Medical prefix (1.2.826.0.1.3680043.10.221) unless the manufacturer of the original image is Phillips, in which case it is changed to a new unique value in the Phillips prefix (1.3.46.670589).
ProtocolName	(0018,1030)	Applies the user provided suffix to the original ProtocolName tag if specified in the app configuration.
StudyDescription	(0008,1030)	Applies the user provided suffix to the original StudyDescription tag if specified in the app configuration.

Table 8: DICOM Metadata Tags Modified by SubtlePET

DICOM Tag Name	Tag Coordinates	Modification by SubtlePET
Series Number	(0020, 0011)	Offsets the original value by 100.
Series Description	(0008, 103E)	Applies the suffix "SubtlePET".
SOPInstanceUID	(0008, 0018)	Changed to a new unique value in the Subtle Medical prefix (1.2.826.0.1.3680043.10.221).
SeriesInstanceUID	(0020, 000E)	Changed to a new unique value in the Subtle Medical prefix (1.2.826.0.1.3680043.10.221).

Table 9: DICOM Metadata Tags Modified by SubtleEDGE

DICOM Tag Name	Tag Coordinates	Modification by SubtleEDGE
PatientsName	(0010,0010)	Anonymize and re-identify PHI/PII tag.
Patient ID	(0010,0020)	Anonymize and re-identify PHI/PII tag.
Patient Birth Date	(0010,0030)	Anonymize and re-identify PHI/PII tag.
OtherPatientIDs	(0010,1000)	Anonymize and re-identify PHI/PII tag.

DICOM Tag Name	Tag Coordinates	Modification by SubtleEDGE
OtherPatientNames	(0010,1001)	Anonymize and re-identify PHI/PII tag.
PatientBirthName	(0010,1005)	Anonymize and re-identify PHI/PII tag.
Patient Size	(0010,1020)	Anonymize and re-identify PHI/PII tag.
Patient Address	(0010,1040)	Anonymize and re-identify PHI/PII tag.
InsurancePlanIdentification	(0010,1050)	Anonymize and re-identify PHI/PII tag.
Patient's Mother's Birth Name	(0010,1060)	Anonymize and re-identify PHI/PII tag.
Military Rank	(0010,1080)	Anonymize and re-identify PHI/PII tag.
Branch of Service	(0010,1081)	Anonymize and re-identify PHI/PII tag.
Medical Record Locator	(0010,1090)	Anonymize and re-identify PHI/PII tag.
Medical Alerts	(0010,2000)	Anonymize and re-identify PHI/PII tag.
Allergies	(0010,2110)	Anonymize and re-identify PHI/PII tag.
Country of Residence	(0010,2150)	Anonymize and re-identify PHI/PII tag.
Region of Residence	(0010,2152)	Anonymize and re-identify PHI/PII tag.
Patient Telephone Numbers	(0010,2154)	Anonymize and re-identify PHI/PII tag.
Ethnic Group	(0010,2160)	Anonymize and re-identify PHI/PII tag.
Occupation	(0010,2180)	Anonymize and re-identify PHI/PII tag.
Smoking Status	(0010,21A0)	Anonymize and re-identify PHI/PII tag.
Additional Patient History	(0010,21B0)	Anonymize and re-identify PHI/PII tag.
Pregnancy Status	(0010,21C0)	Anonymize and re-identify PHI/PII tag.
Last Menstrual Date	(0010,21D0)	Anonymize and re-identify PHI/PII tag.
Responsible Person	(0010,2297)	Anonymize and re-identify PHI/PII tag.
Responsible Person Role	(0010,2298)	Anonymize and re-identify PHI/PII tag.
Responsible Organization	(0010,2299)	Anonymize and re-identify PHI/PII tag.
PatientComments	(0010,4000)	Anonymize and re-identify PHI/PII tag.
Institution Name	(0008,0080)	Anonymize and re-identify PHI/PII tag.
Institution Address	(0008,0081)	Anonymize and re-identify PHI/PII tag.

DICOM Tag Name	Tag Coordinates	Modification by SubtleEDGE
Referring Physician's Name	(0008,0090)	Anonymize and re-identify PHI/PII tag.
Referring Physician's Address	(0008,0092)	Anonymize and re-identify PHI/PII tag.
ReferringPhysicianTelephoneNumbers	(0008,0094)	Anonymize and re-identify PHI/PII tag.
InstitutionalDepartmentName	(0008,1040)	Anonymize and re-identify PHI/PII tag.
PhysiciansOfRecord	(0008,1048)	Anonymize and re-identify PHI/PII tag.
PerformingPhysicianName	(0008,1050)	Anonymize and re-identify PHI/PII tag.
NameOfPhysiciansReadingStudy	(0008,1060)	Anonymize and re-identify PHI/PII tag.
OperatorsName	(0008,1070)	Anonymize and re-identify PHI/PII tag.
AdmittingDiagnosesDescription	(0008,1080)	Anonymize and re-identify PHI/PII tag.
AdmissionID	(0038,0010)	Anonymize and re-identify PHI/PII tag.
RequestingPhysician	(0032,1032)	Anonymize and re-identify PHI/PII tag.
RequestingService	(0032,1033)	Anonymize and re-identify PHI/PII tag.
Unnamed private tag	(0033,1013)	Anonymize and re-identify PHI/PII tag.
Unnamed private tag	(0033,1016)	Anonymize and re-identify PHI/PII tag.
Unnamed private tag	(0033,1019)	Anonymize and re-identify PHI/PII tag.

Subtle Application Private Block

Subtle Medical reserves the private block (0041,00xx) for internal SubtleApp use. The tags in this block are used to store internal debugging information used by Subtle Medical to address image quality issues and trace image transformations. The data in the tags is not intended for third party use and should not be relied upon by third parties. For informational purposes only, the private tags used in that block are:

Table 10: DICOM Tags in the SubtleApp Private Block

DICOM Tag Name	Tag Coordinates	VR	Purpose
SubtleApp Name	(0041, 1001)	LO	Name of the SubtleApp that generated the DICOM
SubtleApp Version	(0041, 1003)	LO	Version of the SubtleApp that generated the DICOM
SubtleApp Model ID	(0041, 1004)	LO	Internal identifier for the underlying AI model used by the SubtleApp
SubtleApp Configuration	(0041, 1005)	LT	The SubtleApp configuration file that was used by the SubtleApp that generated the DICOM

Media Interchange

Not applicable. There is no support for Media Storage Application Profiles because processed images are returned and stored on a customer's device.

Support of Character Sets

All Subtle Medical DICOM applications support:

Table 11: List of Supported Character Encoding Sets

Character Encoding	Code
UTF-8	ISO_IR 192
ISO IR 100 (ISO 1992)	ISO_IR 100
ISO IR 192 (ISO 2002)	ISO_IR 192
ISO IR 100 (ISO 2022)	ISO 2022 IR 100
GB 18030 (GB 2022)	GB18030
GBK (GB 1993)	GBK

Security

SubtleEDGE does not support any specific security measures. It is assumed that SubtleEDGE is used within a secured environment. It is assumed that a secured environment includes at a minimum:

- Firewall or router protections to ensure that only approved external hosts have network access to SubtleEDGE.
- Firewall or router protections to ensure that SubtleEDGE only has network access to approved external hosts and services.
- Any communication with external hosts and services outside the locally secured environment use appropriate secure network channels (e.g. such as a Virtual Private Network (VPN)).

Other network security procedures such as automated intrusion detection may be appropriate in some environments. Additional security features may be established by the local security policy and are beyond the scope of this conformance statement.