DICOM 3.0 Conformance Statement

Butterfly’s Secure DICOM Connector

950-20005-00 rev A

1. Conformance Statement Overview

The DICOM Connector implements the DICOM services to:

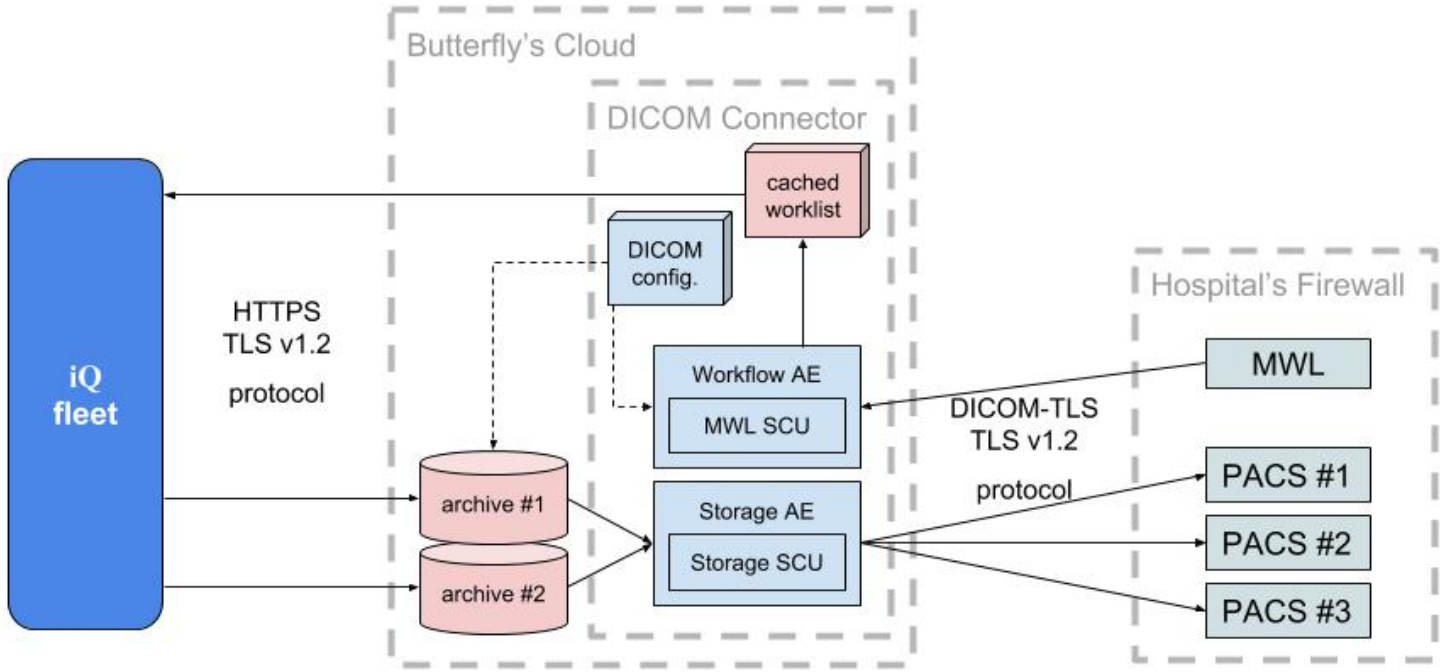
1. Support the Echo (Verification) service as a SCU;
2. Support Modality Worklist Service as SCU;
3. Support Image Storage as SCU;

The following table provides an overview of the network services supported.

SOP Classes	User of Service (SCU)	Provider of Service (SCP)
Transfer		
Ultrasound Image Storage	Yes	No
Ultrasound Multi-Frame Image Storage	Yes	No
Workflow Management		
Modality Worklist (C-FIND)	Yes	No

2. Introduction

The DICOM Connector acts as a hub to centralize the traffic of the iQ's fleet to and from the organization's IT. It behaves like a single ultrasound modality with a DICOM-TLS link to the organization's MWL and PACS. The DICOM Connector lets an administrator configure in one place the DICOM configuration of an entire fleet of iQs.
The DICOM Connector lets an administrator declare up to 16 Image Storage SCP, associate for each archive up to 3 Image Storage SCP and configure one Modality Worklist.



The typical image and loop size are listed below.

Media Type	Compression	Typical size
Single Image	JPEG Lossy	350 kBytes
10-second Loop	MPEG4 / H264	2.7 MBytes

2.1. Revision History

Document Version	Date	Author	Description
00	September, 2018	Damien Dolimier	Initial release

For any other information, or for the latest version of this document, please contact:
Butterfly Network Inc
530 Old Whitfield Street
Guilford, CT 06437
support@butterflynetwork.com
butterflynetwork.com
Service Department
855-296-6188

2.2. Audience

This document is intended for health care system integrators, hospital staff, software developers, etc. A working understanding of the DICOM standards is assumed.

2.3. Remarks

Medical devices implementing subsets of the DICOM Standards are not necessarily interoperable.
This Conformance Statement is an unambiguous specification of the way in which the DICOM Connector implements the DICOM standard. This Conformance Statement is not a replacement for validation of communication with other medical equipment, but provides a first-order check of potential compatibility. The scope of this Conformance Statement is to facilitate communication between the Butterfly probe and other medical equipment.
Several specific issues should be taken into account:
Interoperability: Interoperability of the DICOM Connector with third-party equipment is not guaranteed. Integrating multiple devices in a system depends on the compatibility of the particular implementations of the DICOM standard, as should be described in each Conformance Statement. It is the responsibility of the user to analyze whether devices implementing the DICOM standard meet the application requirements and are able to be integrated.
Validation: While the DICOM Connector is tested to ensure that this Conformance Statement matches the actual implementation, this does not replace the requirement to validate the successful information exchange with medical equipment from other vendors. The user is advised to develop tests that verify information transfer has the required functionality, accuracy and stability before clinical use.
Future evolution of the DICOM Standard: In the future, the DICOM standard may add, deprecate, or change features to meet the needs of users. Butterfly reserves the right to develop our technology and implementation along

with the standard. It is the responsibility of the user to ensure that non-Butterfly equipment also continues to adapt to changes in the standard, as a failure to do so may lead to interoperability issues with the DICOM Connector.

2.4. Definitions and Terms

Full definitions, terms and abbreviations used in this document are defined within the different parts of the DICOM standard.
Some abbreviations are as follows:
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 (AET): the externally known name of an Application Entity, used to identify a DICOM application to other DICOM applications on the network.

2.5. Abbreviations

ACR	American College of Radiology
AE	Application Entity
AET	Application Entity Title
ASUM	Australian Society of Ultrasound Medicine CD-R: Compact Disk Recordable
CR	Computed Radiography
DHCP	Dynamic Host Configuration Protocol
DICOM	Digital Imaging and Communications in Medicine DNS: Domain Name System
FSC	File-Set Creator
FSU	File-Set Updater
FSR	File-Set Reader
HIS	Hospital Information System
HL7	Health Level 7 Standard
IHE	Integrating the Healthcare Enterprise
IOD	Information Object Definition
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standards
JPEG	Joint Photographic Experts Group
LUT	Look-up Table
MPEG	Moving Picture Experts Group
MTU	Maximum Transmission Unit (IP)
MWL	Modality Worklist
NEMA	National Electrical Manufacturers Association NM: Nuclear Medicine
NTP	Network Time Protocol
OSI	Open Systems Interconnection
PACS	Picture Archiving and Communication System PDE: Patient Data Entry
PDU	Protocol Data Unit
RIS	Radiology Information System
SPS	Scheduled Procedure Step
SC	Secondary Capture
SCP	Service Class Provider
SCU	Service Class User
SOP	Service-Object Pair
SPS	Scheduled Procedure Step

TCP/IP	Protocol Transmission Control Protocol/Internet
UID	Unique Identifier
UL	Upper Layer
US	Ultrasound
US MF	Ultrasound Multi-Frame
VR	Value Representation

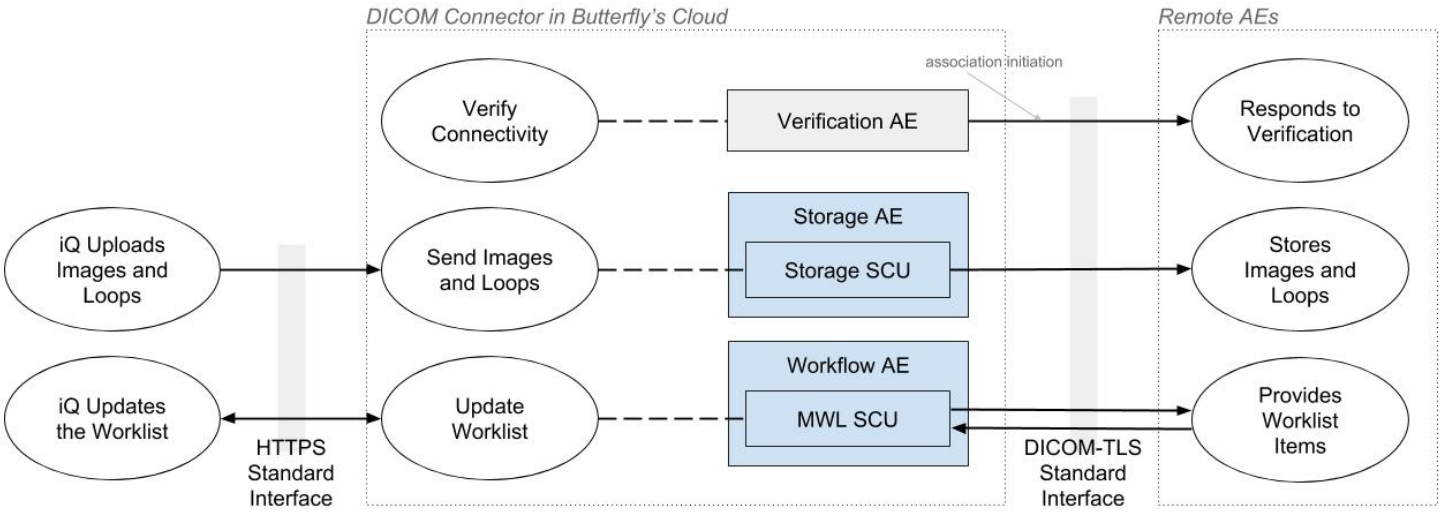
2.6. References

DICOM PS3.1, available at http://medical.nema.org

3. Networking

3.1. Implementation Model

3.1.1. Application Data Flow



3.1.2. Functional Definitions of the Application Entities

3.1.2.1. Storage Application Entity

US Images and US Multiframe Images are sent to a remote AE via the Storage AE. Images are acquired when the user freezes and captures an image while performing an exam, and cines are acquired by recording during an exam. After acquisition, images and cines are uploaded to one of the archive inside the Butterfly Cloud. The complete study is then stored to the PACS associated with this archive. The configuration of the PACS and the association PACS-archive is performed using the Cloud frontend.

3.1.2.2. Workflow Application entity

Worklist information associated with the ultrasound modality is pulled from a remote AE. When associating a patient with an exam, a user may enter data manually or select “Add From Worklist” on the iQ app. One MWL SCP can be

configured and used to pull patient demographics into the Cloud. The Worklist is then cached into the Cloud and broadcasted to the iQ fleet when necessary.
The patient demographics of an exam–pulled from a MWL SCP–once selected cannot be modified by the user to avoid any data reconciliation issue when transferring image data to the remote AEs. In the case when the user enters manually all the patient demographics.

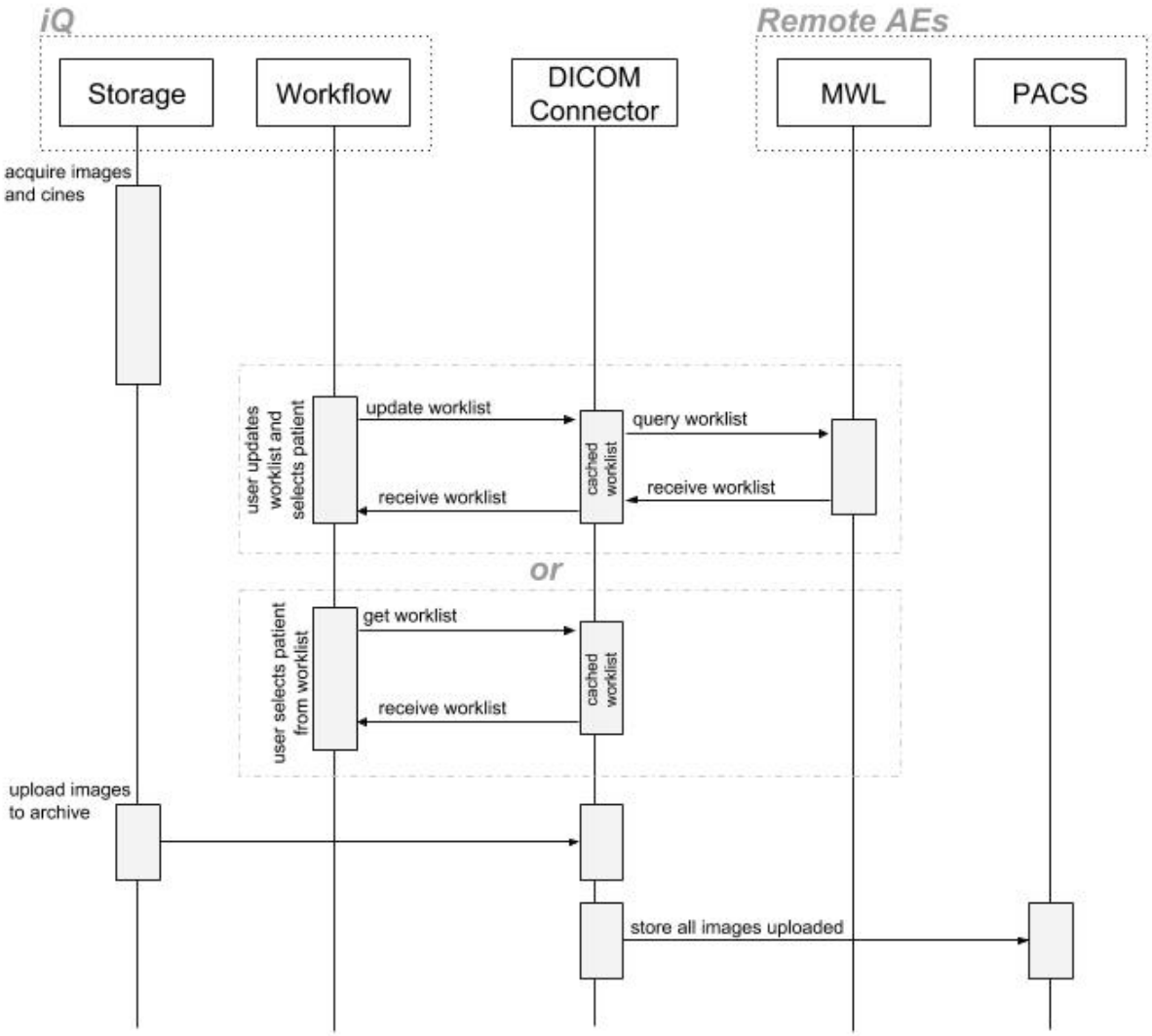
3.1.2.3. Verification

From the Cloud only, a user can verify the connection settings of a MWL or PACS SCP. The DICOM Connector initiates a connection with a remote AE, posts a Verification request and closes the connection.

3.1.3. Sequencing of Real-World Activities

3.1.3.1. Acquisition, Select Patient from Worklist and Upload

This is the sequence of actions for a typical scheduled exam:



3.2. Application Entity Specifications

3.2.1. Storage SCU AE Specifications

3.2.1.1. SOP Classes

SOP Class Name	SOP Class UID	SCU	SCP
US Image Storage	1.2.840.10008.5.1.4.1.1.6.1	Yes	No
US Multiframe Image Storage	1.2.840.10008.5.1.4.1.1.3.1	Yes	No
Video Photographic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.4.1	Yes	No

3.2.1.2. Association Establishment Policy

Application Context Name	1.2.840.10008.3.1.1.1
Maximum number of simultaneous associations	1
Maximum number of outstanding asynchronous transactions	0
Implementation Class UID	1.2.276.0.7230010.3.0.3.6.3
Implementation Version Name	OFFIS_DCMTK_363

3.2.1.3. Association Initiation Policy

3.2.1.3.1. Proposed Presentation Contexts

Abstract Syntax		Transfer Syntax		Role	Extended Negotiation
Name	UID	Name	UID		
US Image Storage	1.2.840.10008.5.1.4.1.1.6.1	Implicit VR Little Endian Explicit VR Little Endian Explicit VR Big Endian JPEG Lossless JPEG Baseline JPEG-LS Lossless JPEG-LS Lossy	1.2.840.10008.1.2 1.2.840.10008.1.2.1 1.2.840.10008.1.2.2 1.2.840.10008.1.2.4.70 1.2.840.10008.1.2.4.50 1.2.840.10008.1.2.4.80 1.2.840.10008.1.2.4.81	SCU	none
US Multiframe Image Storage	1.2.840.10008.5.1.4.1.1.3.1	Implicit VR Little Endian Explicit VR Little Endian Explicit VR Big Endian JPEG Lossless JPEG Baseline JPEG-LS Lossless JPEG-LS Lossy	1.2.840.10008.1.2 1.2.840.10008.1.2.1 1.2.840.10008.1.2.2 1.2.840.10008.1.2.4.70 1.2.840.10008.1.2.4.50 1.2.840.10008.1.2.4.80 1.2.840.10008.1.2.4.81	SCU	none
Video Photographic Image Storage	1.2.840.10008.5.1.4.1.1.77.1.4.1	MPEG4	1.2.840.10008.1.2.4.102	SCU	none

3.2.1.3.2. SOP Specific Conformance for Image SOP Class

This table shows the default settings of timeouts and connection related parameters.

Setting	Default Value	User Configurable
ACSE timeout	30 seconds	yes
DIMSE timeout	300 seconds	yes
Connection timeout	15 seconds	yes
Retry Interval	5 seconds	no
Maximum Retries	3	no

3.2.2. Workflow Application Entity Specification

3.2.2.1. SOP Classes

SOP Class Name	SOP Class UID	SCU	SCP
Modality Worklist Information Model - FIND	1.2.840.10008.5.1.4.31	Yes	No

3.2.2.2. Association Establishment Policy

Application Context Name	1.2.840.10008.3.1.1.1
Maximum number of simultaneous associations	1
Maximum number of outstanding asynchronous transactions	0
Implementation Class UID	1.2.276.0.7230010.3.0.3.6.3
Implementation Version Name	OFFIS_DCMTK_363

3.2.2.3. Association Initiation Policy

3.2.2.3.1. Description and Sequencing of Activity

The request for a Worklist Update is initiated by user interaction from the iQ application. All Modality Worklist operations are performed synchronously and all items are requested. The broad queries are performed using the combination of the following two attributes: Scheduled Procedure Step Start Date (any date or today), Modality (any modality or US).
Remark: this is a very broad query, additional query capabilities are implemented in the iQ application to select in a very efficient way the right patient demographics.
For each query of a remote application entity for a Modality Worklist list of items, the DICOM Connector initiates an association, sends a C-FIND request command, waits in blocking mode for all C-FIND responses, and then releases

the association. A possible sequence of interactions between the Workflow AE and a Departmental Scheduler (e.g. a device such as a RIS or HIS which supports the Modality Worklist SOP Class as a SCP) is illustrated in Figure 3.2.3:
1. The Workflow AE opens an association with the Departmental Scheduler;
2. The Workflow AE sends a C-FIND request to the Departmental Scheduler containing the Worklist Query attributes;
3. The Departmental Scheduler returns a C-FIND response containing the requested attributes of the first matching Worklist Item;
4. The Departmental Scheduler returns another C-FIND response containing the requested attributes of the second matching Worklist Item;
5. The Departmental Scheduler returns another C-FIND response with status Success indicating that no further matching; Worklist Items exist. This example assumes that only 2 Worklist items match the Worklist Query;
6. The Workflow AE closes the association with the Departmental Scheduler;

3.2.2.3.2. Proposed Presentation Contexts

3.2.2.3.3. SOP Specific Conformance for Worklist Management SOP Class

Module Name >Attribute Name	Tag	Matching Keys for Work List Update	Matching Keys for Work List Search	Editable in Patient Form	Displayed in Work List	Copied into Image IOD
Scheduled Procedure Step:						
Scheduled Procedure Step Sequence	(0040,0100)	-	-	-	-	-
>Scheduled Station AE Title	(0040,0001)	-	-	-	-	-
>Scheduled Procedure Step Start Date	(0040,0002)	range	-	-	-	-
>Scheduled Procedure Step Start Time	(0040,0003)	range	-	-	-	-
>Scheduled Procedure Step Location	(0040,0011)	-	-	-	-	-
>Modality	(0008,0060)	value	-	-	-	yes
>Scheduled Performing Physician's Name	(0040,0006)	-	-	-	-	-
>Scheduled Procedure Step ID	(0040,0009)	-	-	-	-	yes
>Scheduled Protocol Code Sequence	(0040,0008)	-	-	-	-	yes
>>Code Value	(0008,0100)	-	-	-	-	yes
>>Coding Scheme Version	(0008,0103)	-	-	-	-	yes
>>Coding Scheme Designator	(0008,0102)	-	-	-	-	yes
>>Code Meaning	(0008,0104)	-	-	-	-	yes
>Scheduled Procedure Step Description	(0040,0007)	-	-	-	-	yes
Requested Procedure:						

Requested Procedure Description	(0032,1060)	-	-	-	-	yes
Requested Procedure Code Sequence	(0032,1064)	-	-	-	-	yes
>Code Value	(0008,0100)	-	-	-	-	yes
>Coding Scheme Designator	(0008,0102)	-	-	-	-	yes
>Coding Scheme Version	(0008,0103)	-	-	-	-	yes
>Code Meaning	(0008,0104)	-	-	-	-	yes
Requested Procedure ID	(0040,1001)	-	-	-	-	yes
Study Instance UID[2]	(0020,000D)	-	-	-	-	yes
Referenced Study Sequence	(0008,1110)	-	-	-	-	yes
>Referenced SOP Class UID	(0008,1150)	-	-	-	-	yes
>Referenced SOP Instance UID	(0008,1155)	-	-	-	-	yes
Imaging Service Request:						
Accession Number[1]	(0008,0050)	-	yes	yes	yes	yes
Requesting Physician	(0032,1032)	-	-	-	-	yes
Referring Physician's Name	(0008,0090)	-	-	-	-	yes
Visit Identification:						
Admission ID	(0038,0010)	-	-	-	-	-
Visit Status:						
Current Patient Location	(0038,0300)	-	-	-	-	-
Visit Relationship:						
Referenced Patient Sequence	(0008,1120)	-	-	-	-	yes
>Referenced SOP Class UID	(0008,1150)	-	-	-	-	yes
>Referenced SOP Instance UID	(0008,1155)	-	-	-	-	yes
Patient Identification:						
Patient's Name[1]	(0010,0010)	-	yes	yes	yes	yes
Patient ID[1]	(0010,0020)	-	yes	yes	yes	yes

Patient Demographic:						
Patient's Birth Date[1]	(0010,0030)	-	-	yes	yes	yes
Patient's Sex[1]	(0010,0040)	-	-	yes	yes	yes
Confidentiality constraint on patient data	(0040,3001)	-	-	-	-	-
Patient Medical:						
Patient State	(0038,0500)	-	-	-	-	-
Pregnancy Status	(0010,21C0)	-	-	-	-	-
Medical Alerts	(0010,2000)	-	-	-	-	-
Additional Patient History	(0010,21B0)	-	-	-	-	-
Allergies	(0010,2110)	-	-	-	-	-
Patient's Weight	(0010,1030)	-	-	-	-	-
Patient's Size	(0010,1020)	-	-	-	-	-
Special Needs	(0038,0050)	-	-	-	-	-
Requested Procedure Comments	(0040,1400)	-	-	-	-	-
Last Menstrual Date	(0010,21D0)	-	-	-	-	-

note 1: In the case of a patient demographics import from the worklist, the DICOM tag value may not be modified by the iQ app user. This field is read-only. In the opposite case–unscheduled workflow–this field may be entered by the user.
note 2: In the case of a patient demographics import from the worklist, the DICOM tag value may not be modified by the iQ app user. This field is read-only. In the opposite case–unscheduled workflow–this field is automatically generated to guarantee its uniqueness.

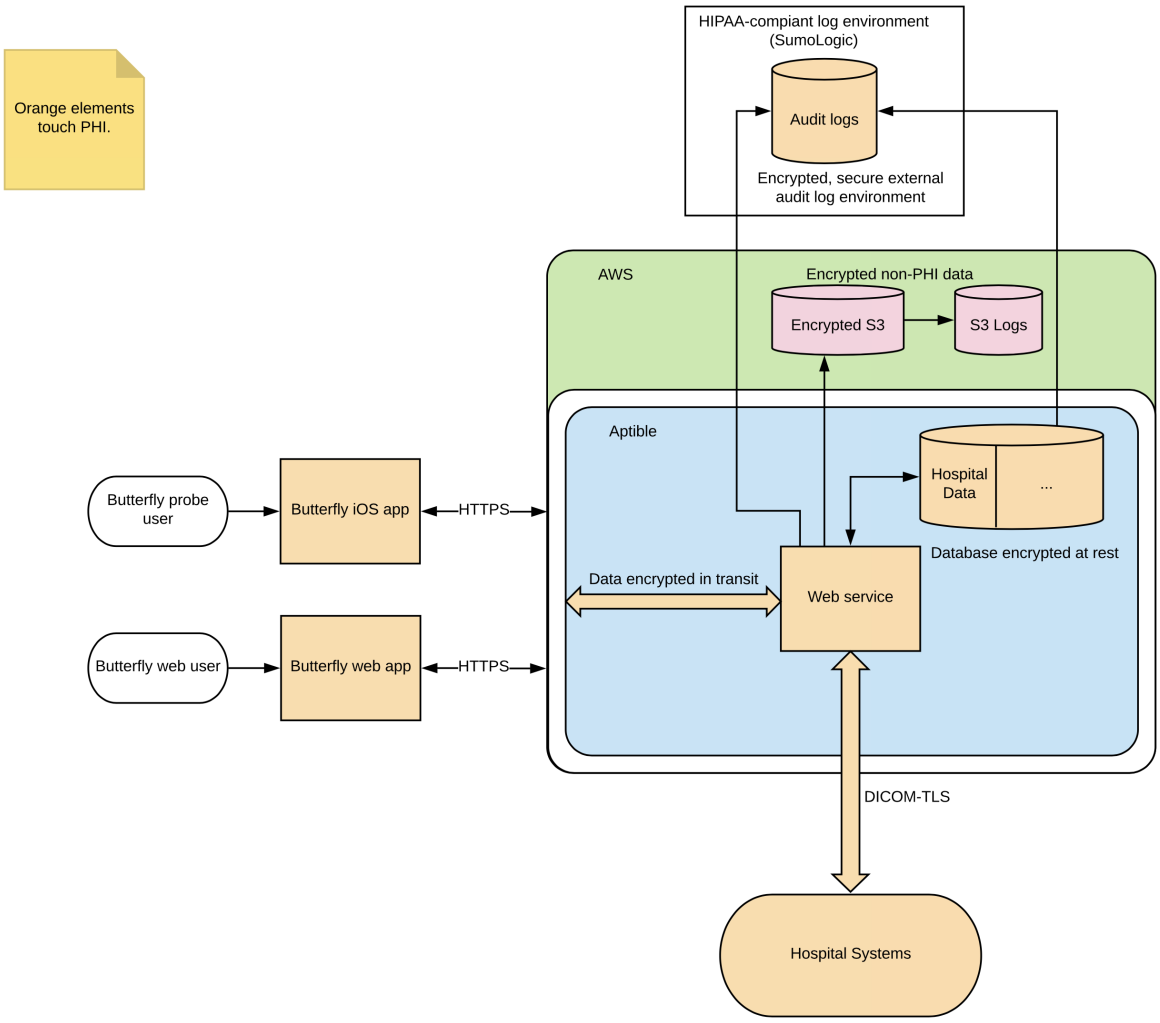
4. Support of Extended Character Sets

The following character sets are supported for both the storage and workflow entities.

DICOM	Character Set	Coverage
ISO_IR 6	ASCII	
ISO_IR 100	Latin alphabet #1	Afrikaans, Albanian, Breton, Catalan, Danish, English (UK and US), Faroese, France, Galician, German, Ice- landic, Irish (new orthography), Italian, Kurdish (The Kurdish Unified Alphabet), Latin (basic classical orthography), Leonese , Luxembourgish (basic classical orthography), Norwegian (Bokmål and Nynorsk), Occitan, Portuguese (Portuguese and Brazilian), Rhaeto-Romanic, Scottish Gaelic, Spanish, Swahili, Swedish, Walloon, Basque
ISO_IR 192	Unicode	

5. Security

High level diagram of the security-related partners with Butterfly:



5.1. DICOM security good practices

This supplement 204 – TLS Security Profiles contains the latest recommendations about the recommended cypher suites to use in the case of a secure DICOM-TLS connection.
http://dicom.nema.org/Dicom/News/September2017/docs/sups/sup204.pdf

How to Increase the Security of DICOM Servers
http://www.medicalimagingtalk.com/diagnostic-imaging/how-to-increase-the-security-of-dicom-servers/

5.2. HITRUST, SOC II and HIPAA compliance

The Butterfly Cloud uses the built-in capabilities of Amazon's AWS, Aptible and auth0 to ensure security during the authentication phase, transmission and at rest. These three companies are certified:

Aptible is HITRUST and SOC II-certified:
https://www.aptible.com/compliance/hitrust-csf-certification/
https://www.aptible.com/blog/aptible-soc-2-type-2-report-now-available/

AWS is HIPAA-compliant:
https://aws.amazon.com/blogs/apn/hipaa-and-hitrust-on-aws/

Auth0 is SOC II-certified and HIPAA-compliant:
https://auth0.com/security

6. Appendix

6.1. DICOM Configuration

The DICOM configuration of each device is not necessary since all the iQ devices upload the acquired images to the Butterfly Cloud. This mode of operation allows a simple and efficient management of the fleet of iQs. From a DICOM perspective, the Butterfly Cloud and its DICOM connector is a single virtual ultrasound system to configure and declare to your existing PACS and MWL.
Please go to the DICOM Administration page in the Butterfly Cloud, please note that an administrator account is required to access and modify the DICOM configuration.

6.2. Existing PACS and MWL Service Providers

In order to facilitate the DICOM configuration in the Butterfly Cloud, please complete the tables below.

DICOM PACS (Store SCP)

Vendor name, Model, Revision number	
AET	
External Hostname / IP	
External Port number	
Character encoding *ISO IR100, ISO IR6 and ISO IR192 are supported*	
Preferred Image Compression *Uncompressed, JPEG Lossy, JPEG Lossless, JPEG LS Lossy, JPEG LS Lossless are supported*	
Preferred Multi-Frame Compression *Uncompressed, JPEG Lossy, JPEG Lossless, JPEG LS Lossy, JPEG LS Lossless, MPEG4 US Multiframe Image Storage and MPEG4 Video Photographic Image Storage are supported*	

DICOM MWL (Find SCP)

Vendor name, Model, Revision number	
AET	
External Hostname / IP	
External Port number	
Character encoding *ISO IR100, ISO IR6 and ISO IR192 are supported*	

6.3. New Service Users

6.3.1. Storage SCU - Butterfly's Cloud Virtual Modality

calling AET	
CA Certificate (pem format)	

6.3.2. Worklist SCU - Butterfly's Cloud Virtual Modality

calling AET	
CA Certificate (pem format)	

6.4. Tasks

6.4.1. Network/Security Administration

- Open 2 ports on the organization's firewall to authorize the incoming traffic from the Storage SCU and Worklist SCU (if applicable).
    - Please filter the incoming connections for the Butterfly Cloud. The IP address will be provided during implementation.
- Declare and authorize, on the Storage SCP, a new calling AET for the Butterfly's Cloud Storage SCU.
- If applicable, declare and authorize, on the MWL SCP, a new calling AET for the Butterfly's Cloud MWL SCU.
- Generate a CA certificate to authenticate the SCP, this certificate will be uploaded to the Butterfly Cloud. The certificate can be the same of different for the Store and MWL SCP.
    - Please note that this step is not necessary for Telexy's QPath Classic PACS. Just specify in the TLS Security field the use of QPath Classic.
- Download the Butterfly Cloud's certificate for your organization to authenticate the SCU, this step is optional but should be configured to add extra security the authentication process.
- If using WiFi for the iQ, be sure to connect your Butterfly iQ devices to an internet-facing network.

6.4.2. Butterfly Cloud Setup

- Log in to the Butterfly's Cloud using an account with administrator privileges.
- Go to the DICOM Administration page.
- Add a PACS and fill in the parameters using the table above. You may want first to verify the connection–if the Storage SCP accepts an unsecured connection–with no security selected.
- Save the settings.
- On the main DICOM administration page, verify the settings with the Echo button.
- Perform the same tasks to configure the Worklist System. Please note that only one Worklist can be configured and added per organization.
- Associate the PACS to an archive.

---------- End of Document ----------