MediCal QAWeb Security and Privacy Statements

1.1. INTRODUCTION

The uptime of your PACS workstations is critical for the productivity of your radiology department. Barco's MediCal QAWeb is the industry's first secure online that guarantees maximum use of your PACS displays by providing automated DICOM Calibration with display asset management.
Since the major renewal in this concept is the "online service" a lot of security and privacy questions rise, and indeed these are valid concerns. This document highlights and describes all these concerns by explaining the MediCal QAWeb architecture and its features ensuring a solid and secure solution is provided.

1.2. BASED ON A SECURITY AND PRIVACY REQUIREMENTS FROM NEMA[1]

MediCal QAWeb is designed based on the document "Security and Privacy Requirements for Remote Servicing" [2] from the NEMA organization. This paper lists a number of requirements about security and privacy concepts and security technology that relate to modern healthcare data security and data privacy regulations.
In this document (which is publicly available on the internet – look at the references at the end of this document) we will refer to this original paper (the text in italics) and based on that the approach for QAWeb will be explained.

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

1.2.1. Paper header and introduction

The white paper "Security and Privacy: An Introduction to HIPAA" by NEMA MII Security and Privacy Committee discusses security and privacy concepts and security technology that relate to modern health care data security and data privacy regulations. Risk assessment and risk mitigation are explicitly mentioned in the US HIPAA regulations and should be conducted in many other countries. This paper describes how the risks that could be correlated with remote servicing may be reduced.

MediCal QAWeb comment:
In healthcare NEMA is accepted as being the reference for guidelines and standards. There is no legal document or certification that can state that a product is HIPAA compliant, this NEMA standard document very well highlights all possible risks and their mitigations, if MediCal QAWeb complies to all these, this solution should be validated and accepted.

1.2.2. Remote Servicing: New Servicing Possibilities

Medical equipment in health care facilities is becoming increasingly sophisticated. On the one hand the growing complexity of hardware and the increased functionality of firmware or software require vendor-specific knowledge for maintenance or repair. On the other hand, an increasing number of these medical systems are connected to hospital internal networks which themselves are becoming increasingly likely to be linked to the worldwide Internet. Thus, software-related maintenance or repair could be conducted by servicing staff located in a servicing center at a location remote from the health care facility itself. In this way certain types of equipment maintenance and repair could be performed without requiring a personal visit by a service technician.

MediCal QAWeb comment:

The PACS workstations are key components in realizing these goals. Barco's display systems (PACS displays and graphic controllers) are of major importance for the daily work of every radiologist. MediCal QAWeb continuously monitors (local only through the MediCal QAWeb Agent) the health of these display systems and notifies the right persons when a possible issue is detected.

Remote servicing offers customers several advantages. The most important would be that maintenance or repair response times could be reduced, and availability of equipment increased. Additionally, remote servicing could result in lower costs for customers since on-site maintenance visits would be reduced. Furthermore, innovative services could be offered, e.g., scheduled pre-emptive maintenance to avoid unplanned accidental downtime.

MediCal QAWeb comment:

MediCal QAWeb allows very fast issue identification and suggests corrective actions for the end user. The service provider for the medical displays can also

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

access the issue data (through the secured online service), and if necessary a Barco support engineer can review the details. This indeed will result in a maximum uptime of your medical workstation.

However, legislative initiatives and good security practice both require that access to Protected Health Information (PHI), that identifies medical and other personal facts belonging to a specific patient, be controlled to prevent a compromise of its confidentiality or integrity during remote or local system servicing. This white paper suggests an architecture that, if implemented, can create and maintain a trust relationship between vendors and health care institutions. It presents a secure methodology for protecting PHI, in accordance with international healthcare data security and privacy regulations, during remote servicing. It does not contain concise definitions or mandatory guidelines, but instead outlines the main components of a secure remote servicing capability that can satisfy security and privacy concerns while allowing cost-effective remote maintenance and repair of medical information systems.

MediCal QAWeb comment:
Although MediCal QAWeb does not collect any PHI, it is based on the suggested architecture to ensure this trust relationship between vendors and medical facilities.

1.2.3. A Secure Remote Servicing Information Technology Architecture

The example of a secure Information Technology (IT) architecture for remote servicing suggested by this white paper is illustrated in Figure 1. Remote Servicing Centers (RSCs) of different vendors are located outside of the health care facilities in which their products, owned by their customers, are installed. Access, via wide area network, dial-up, or persistent communication lines to the local network of the different health care facilities is granted at a single, well-defined access point. The single access point into the health care facility, for use by the RSCs of all vendors, would simplify the network and security management tasks of a customer's IT administrator. Each RSC would be granted access only to the equipment it was authorized to maintain or service in the internal network even if several modalities, originating from many vendors, are present.
To control costs and keep the implementation as open as possible, off-the-shelf technology, e.g., routers and firewalls, are envisioned being used to the maximum practical extent. Customized solutions would be minimized or eliminated.

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

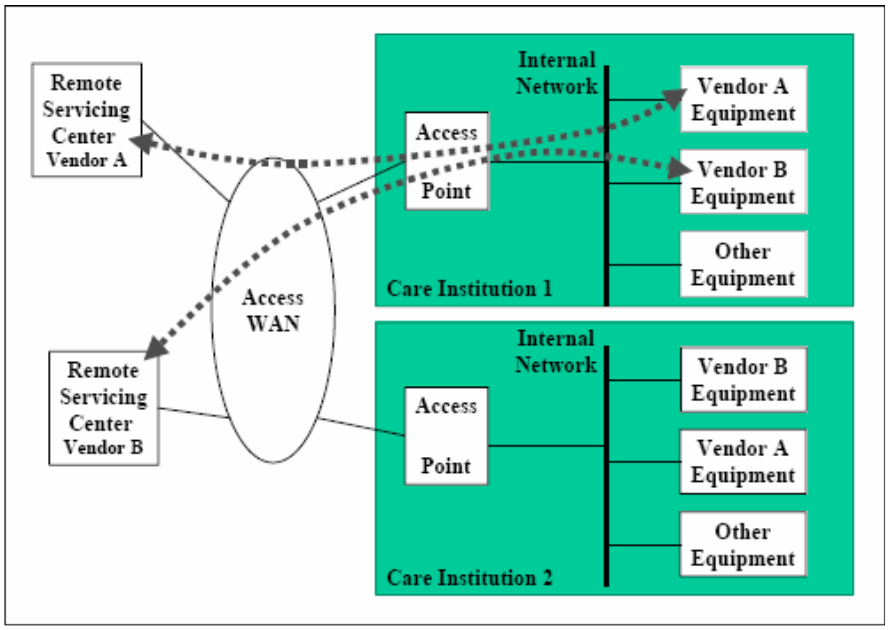

Figure 1 – A remote Servicing IT Architecture

MediCal QAWeb comment:

As shown in Figure 1A, the suggested IT architecture is used by MediCal QAWeb, the vendor equipment is represented by the PACS workstation, containing Barco's medical displays and graphic controllers. They are connected to the internal network of the facility, without open connectivity to the outside or a WAN. The QAWeb Agent is based on a local service enabling automatic calibration and compliance of the display systems towards internationally accepted quality assurance guidelines.

The Access Point is represented by the QAWeb Relay, a PC protected by firewall(s) running specific QAWeb software for internal/external secured communication. The service centre is within QAWeb represented by the MediCal QAWeb server – residing in a well protected area – and a possible remote user. All asset and QA data resides on the QAWeb server and can be accessed by an authorized remote user through a secure connection. Every medical facility has its own QAWeb Relay and its connectivity to the internet.

Different – and even stricter – in QAWeb is the fact that the QAWeb Relay is not really directly accessible by a remote user. It is always the QAWeb Relay taking the initiative to initiate a request to the QAWeb server for a possible action. This means that only outbound, secured traffic through https (port 443) has to be enabled from the QAWeb Relay to the internet. Remote requests are validated and further processed by the QAWeb Relay before they reach the internal network. It is the QAWeb Agent that polls on a regular timeframe the QAWeb Relay for these requests. At that time, these are gathered by the right Agent and a real action is executed.

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

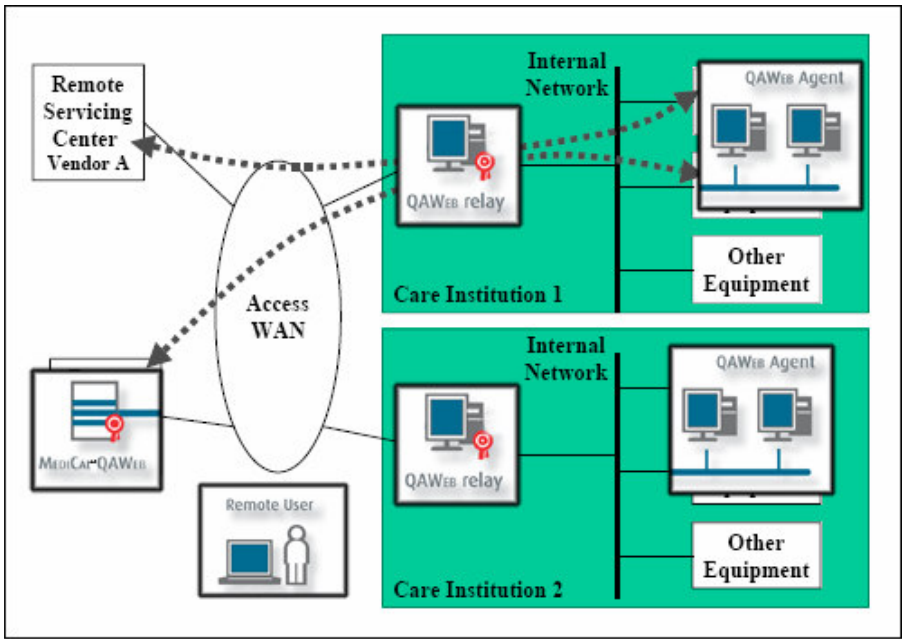

Figure 1A – How MediCal QAWeb's Architecture fits to this

Figure 1B shows the same MediCal QAWeb architecture as a total picture. Her only one facility is shown, but this concept is designed for multiple facilities each with its own QAWeb Relay. The small marks next to every workstation represent a certificate that is used, the red double lines represent a firewall.
A technical document about the details of this concept is added in Appendix A.

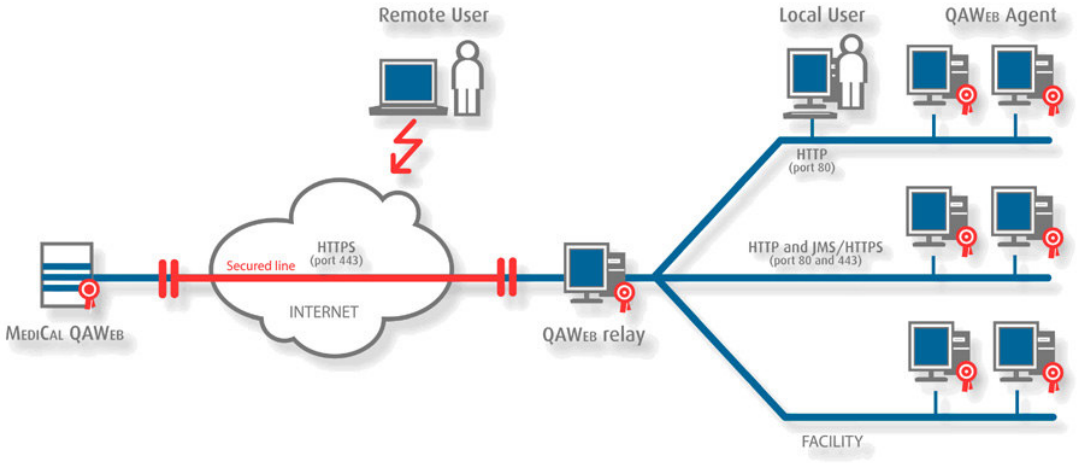

Figure 1B – Concept Overview of QAWeb Server, Relay and Agent

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

1.2.4. Remote Servicing Security and Privacy

Regardless of whether the servicing staff is present at the modality or located in a RSC, the same level of security and privacy is required and can be realized. Although the general goals for data security and privacy – availability, confidentiality, and integrity – are unchanged the measures to be taken to realize them differ when performing remote servicing. During many types of RSC sessions, PHI access is unnecessary, e.g., retrieving calibration information. In principle such sessions would not require specific PHI-protective security measures. However, the same level of security safeguards should be applied in all cases to meet legislative mandates, establish a vendor-customer trust relationship, and simplify the service interface.

MediCal QAWeb comment:

A local user, inside the medical facility, can easily access the QAWeb Agent, and if necessary also the QAWeb Relay. The same person can also review and manage all assets using a web interface from within the facility. The application data is workstation information, display information and graphic controller information. It does not contain any PHI. But still all proper security safeguards are applied in all cases. A QA technologist can be notified or paged for a possible issue even when he is not physically inside the facility. In that case he uses the same service interface for ensuring the fastest possible corrective action.

1.2.4.1. Establishing the Connection

The basic need of the health care facility is to insure it knows to its satisfaction who is accessing its equipment. This must be accomplished by the customer first identifying and then authenticating the claimed identity of the RSC that is attempting to connect with the customer's equipment before access is granted to its facilities, its network, or the vendor system. Health care facilities do not need to individually identify and authenticate RSC service technicians themselves because they would already have been identified and authenticated by vendor IT at the RSC. This approach avoids the need for each health care facility to maintain lists of authorized service technicians from each of their vendors.

The architecture illustrated in Figure 1 calls for the use of a strong authentication mechanism between the RSC and the health care facility access point. This mechanism might use one or another of several techniques or technologies, such as electronic certificates, automated or manual telephone callback, authentication tokens, single-use authentication, or call line identification. The method ultimately chosen will depend on the perception of risk to be controlled, in accordance with results of its analysis. In this way health care facilities can significantly reduce the probability of falling victim to a fraudulent attempt by an unauthorized entity to be connected to its internal network or systems.

MediCal QAWeb comment:

MediCal QAWeb contains a user database for every medical facility. A user has to identify himself and needs authentication before any information can be accessed. The application uses different roles for internal – facility users – and remote users as the service provider or Barco. All users are stored at one location – in the QAWeb server – and all facility users can be managed by the

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

radiology manager (or the person with administrative privileges in QAWeb for its facility), this enables an easy user and identity management for local and external users. All login actions are logged in the QAWeb server and a monthly activity report is sent to the radiology manager containing the persons who logged in and the number of logins during the last month.
The communication between the QAWeb Relay (initiator!) and the QAWeb server is indeed based on strong authentication based on Public Key Infrastructure (PKI) and 128 bit encryption.
Also the QAWeb Relay keeps a log of all outgoing/incoming requests which can be consulted from within the facility, only at the QAWeb Relay machine itself. These mechanisms ensure an easy to use application in a highly secured environment.

1.2.4.2. Access to Systems Requiring Remote Service

After the RSC is authenticated to the health care facility at its single access point, only specific addresses and protocols (such as ftp, http, https) required by the particular vendor would be authorized for use. In this way RSC service technicians could connect only to specific systems on the health care facility local area network. The health care facility ultimately has control and provides the RSC only with the access rights necessary to perform approved tasks. Health care facilities may have many systems in their local network. Thus an additional authentication procedure via RSC-ID and password should be implemented at the vendor system itself that is being serviced. This will enable another level of authorization and accountability.

MediCal QAWeb comment:

Every facility QAWeb user logging in onto the QAWeb Server can only access information about its own specific healthcare organization. The MediCal QAWeb Relay is also a dedicated machine for this purpose and this vendor, using this PC for other purposes should happen with care (not encouraged since it can involve a higher risk towards security breaches).
No other user or application from the WAN or internet can access the QAWeb Relay or the access point since it is the Relay itself only talking to the well identified QAWeb server.
QAWeb uses one resource for all QAWeb users (the QAWeb server) and so authentication is easy to manage.

1.2.4.3. Manual Disconnection

Policy, procedures, and technology at the RSC will dictate allowable actions during remote servicing to ensure that all maintenance and service activities are authorized. That withstanding, there may be cases where a knowledgeable person at the health care facility may want to monitor and ultimately terminate an on-going RSC session. Due to the potential complexity of remote servicing, the technology needed to enable monitoring in a meaningful way can vary. Monitoring might be possible using specific equipment or applications, or by simple data traffic analysis. Should the health care facility decide to disconnect an RSC session, its decision must be based on well-defined policies and

procedures, to protect against compromising the stability, availability, and integrity of its health care systems.

MediCal QAWeb comment:

Since softcopy quality assurance really works and has added value if it can happen intervention free and transparent to the workstation end user (radiologist), most actions for remote servicing will not really result in visual changes. And if this is the case – in case QAWeb changes a setting on a display system – the QAWeb Agent will always notify this or allows this action at a time no user is in front of the workstation.

These actions are however all logged at 2 levels for the facility users: first of all at the QAWeb Relay and secondly at the QAWeb Agent. For more information we refer to the next topic about log files.

1.2.4.4. Log Files

Log files of all security-relevant activity during each RSC session must be created, stored and protected. The architecture illustrated in Figure 1 implies that separate log files should be created and maintained at:

- *The RSC itself.*
- *The health care facility access point.*
- *The vendor system being serviced.*

At the RSC the identification and authentication of servicing staff and its activity must be logged. The health care facility access point must store data about when and to whom access was granted, and the identification of the vendor system being serviced. Finally, the vendor system being serviced should record – to the extent possible and based upon the nature of the service being performed – all servicing accomplished and by whom.

All of these log files are components of a broad audit control infrastructure, itself an important part of the authentication and authorization tracking mechanism. Audit logs and the mechanisms of using them are specifically covered in a companion document to be published soon by NEMA MII Security and Privacy Committee entitled "Audit Controls". This document covers not only the content of audit logs, but their protection, their mining and maintenance, and how long these audit trails need to be maintained.

MediCal QAWeb comment:

Logging is indeed enable at different levels:

a) The MediCal QAWeb server keeps all log information local in a secured environment. If necessary logging information can be requested to Barco for a specific facility and or action.

b) Secondly the access point or QAWeb Relay also keeps track of all outgoing/incoming requests for its facility. This is also stored locally on this machine and can only be accessed by an administrative user of that machine. This – in combination with the monthly activity reports – identifies the actual users and local and remote activity of this secured solution. These logs are never cleared by the application or systems, but can of course be manually removed.

c) At the third level the QAWeb Agent also keeps track of all local activity: what was executed when. Combine this with a lot of reports that can be consulted

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

from the QAWeb interface: workstation reports, display reports, issue reports, …

MediCal QAWeb supports an extensive list of logging activities ensuring the highest level of confidence for every user.

1.2.4.5. Secure Data Transfer

All data transmitted between the RSC and the health care facility must be treated as confidential unless there can be legal certainty that no PHI will be carried. There are two ways to provide the required protection: physical protection of the communication channel itself or encryption of the data. If communication lines cannot be protected by physical means, then many encryption technologies, e.g., VPN, IP-Sec, SSL, application-level encryption, are available to protect data confidentiality (and, incidentally, its integrity). The encryption technique chosen must be adequate to protect against known and anticipated threats. For example, a VPN established between the RSC and the health care facility access point can provide protection of the data while on an open network such as the Internet, assuming physical security or encryption is available to protect data on RSC or health care facility internal networks.

MediCal QAWeb comment:

Although MediCal QAWeb does not transfer any PHI, it implements 128 bit encryption on SSL between the QAWeb Relay and the QAWeb server. The QAWeb Relay is not reachable from the outside, only outbound, secured https traffic is allowed on the firewall between the QAWeb server and the Relay.

1.2.4.6. Organizational Policies and Procedures

Performing authorized remote servicing can result in the intentional or accidental download of PHI into the RSC. RSC operators and health care facility operators both have a legal duty to protect PHI against compromise of its confidentiality. It will be necessary, therefore, for specific privacy-preserving policies and procedures to be developed, implemented, enforced and maintained by RSCs. Development or enforcement might call for:

- *Evidencing employee understanding of the need to protect any PHI they come in contact via a signed, written internal agreement.*
- *Secure disposal of PHI and other records when no longer needed.*
- *Mechanisms at the RSC to control and record access to and dissemination of any PHI collected or retained.*
- *Conducting maintenance work using de-identified health information whenever possible.*

MediCal QAWeb comment:

MediCal QAWeb never transfers, downloads or communicates PHI, not in the healthcare facility, nor outside the facility. If however a workstation is shipped outside the facility to a vendor, this is indeed applicable and HIPAA regulations are applied. Barco's approach to this is described in our white paper, included in this document as Appendix B.

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

1.2.5. Privacy is the Goal and Security the Way

Protecting personal health care information has always been important to healthcare facilities and vendors. As health care is extending into the information age we all must examine and improve our privacy enforcing policies, procedures, and technologies. The example of remote servicing shows that as a pre-requisite both parties, the health care facility and the vendor, have to secure their local networks.

Together with the remote servicing architecture presented herein vendors and healthcare facilities can provide a secure capability for customer-oriented servicing. Eventually this innovative servicing can be conducted at the same level of security and privacy as if the servicing staff were physically present on-site.

MediCal QAWeb comment:

It is clear the MediCal QAWeb is based on this NEMA guideline, and that it goes beyond its requirements ensuring a trustful relationship between vendor and healthcare facility

1.3. CONCLUSIONS

The internet boom has made life easier for a lot of people and especially for the medical imaging industry. In the last couple of years the benefits of this technology have overcome the security concerns. Device management and remote support are commonly installed features in healthcare.

Based on the above realizations of the requirements, it is clear that MediCal QAWeb is superior to minimize security and privacy risks in all ways.

The technology used for MediCal QAWeb is based on state-of-the-art security concepts. It is also based on the current security standards and flexible for any new standard to be implemented in the future.

This technology is indeed the first in the market for softcopy QA, it ensures a higher uptime for the medical workstation and will make the life easier of a lot of QA technologists in the field.

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457

2. APPENDIX A: MEDICAL QAWEB SECURITY ARCHITECTURE

This document is a separate file and will be distributed accordingly.

3. APPENDIX B: HOW BARCO ADDRESSES HIPAA

This is also a separate document and is available on the internet.

References:

[1] www.nema.org
[2] http://medical.nema.org/privacy/remote.pdf

Barco n.v.
President Kennedypark 35
B-8500 Kortrijk, Belgium
Tel.: +32 56 233 211 - Fax: +32 56 233 457