

Security and Privacy Requirements for Remote Servicing

A Paper by:

The Security and Privacy Committee

Medical Imaging Informatics Section



April 26, 2001

Security and Privacy Requirements for Remote Servicing

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.

1. 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 requires 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.

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 preemptive maintenance to avoid unplanned accidental downtime.

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.

2. 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

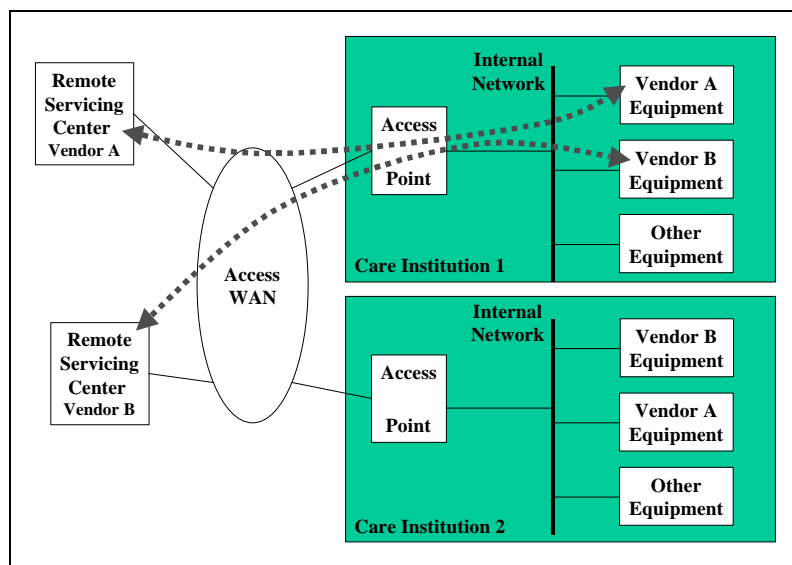


Figure 1: A Remote Servicing IT Architecture

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.

3. 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.

- *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 call-back, 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.

- *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.

- *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.

- *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.

- *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.

- *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.

4. 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.