

Remote Services in Healthcare – Use Cases and Obligations For Customer and Service Organizations

This White Paper was developed by the
Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC)

The White Paper has been approved by:
MITA (Medical Imaging & Technology Alliance, a division of NEMA)
COCIR (European Coordination Committee of the Radiological and
Electromedical Industry)
JIRA (Japan Industries Association of Radiological Systems)

September 2008

© JOINT NEMA/COCIR/JIRA SECURITY AND PRIVACY COMMITTEE (SPC)
www.medicalimaging.org
Secretariat: MITA (Medical Imaging & Technology Alliance)
1300 North 17th Street, Suite 1752, Arlington, VA 22209, USA
tel: 001-703-841-3200, fax: 001-703-841-5900
Secretary: Richard Eaton, tel: 001-703-841-3248, fax: 001-703-841-3348
E-mail to: reaton@medicalimaging.org

May be quoted if reference and credit to SPC is properly indicated.

Table of Contents

1. Introduction	3
2. Use cases	4
2.1 On-demand services	4
2.2 Routine services	5
3. Boundaries on remote service.....	6
3.1 International aspects.....	6
3.2 Risks related to remote services.....	6
4. Access to patient data.....	8
4.1 Remote maintenance without access to patient data.....	8
4.2 Access to patient data: possible or even required.....	8
5. Technical and organizational solutions around remote service ..	8
5.1 Organizational policies and procedures	9
5.2 Technical Practices.....	9
5.3 Recommended responsibilities in technical practices	11
6. Conclusion	12

1. Introduction

Medical equipment increasingly relies on information technology (IT). Film-based medical imaging has waned as information technology (IT) has become dominant in the collection, distribution, viewing, and storage of diagnostic information. Among the many productivity-enhancing features of IT is the ability to effectively leverage network connections to provide remote service to hardware and software allowing for increased uptime and added-value services. Remote service is defined as the delivery of hardware and/or software system maintenance from a location beyond the healthcare delivery organization's system operating site (generally via an external telephone carrier or digital network provider connection).

Remote service ability has become part of standard installations of equipment. Over the last few years it has evolved from early remote diagnostic tools (used to provision service technicians with needed parts prior to arriving on site) to comprehensive, remote maintenance services. Today, a manufacturer's remote service portfolio provides a menu of applications including look-over-the-shoulder assistance, business-specific value-added services, and proactive diagnostics. Typical automated messages carry status information that may contain early indication of a possible system condition which, if allowed to worsen, would result in sudden and unexpected system problems resulting in unavailability. All these services are performed from vendors' service centers which may be located at different sites around the world.

The benefits of remote services are obvious for both customers and manufacturers. They reduce and often eliminate travel time and significantly reduce service costs, thus increasing the productivity of the high technology equipment in hospitals. Customers, recognizing these benefits, have accepted and embraced this service innovation. Nonetheless, customers are increasingly concerned about possible data privacy and data security issues that are encountered when connecting their patient care and diagnostic systems to external remote servicing centers. Hence, securing the information flow in the provision of remote access is critical to maintaining information protection and to maintain customer trust in these innovative technologies.

This White Paper describes a set of use cases that include associated data security and data privacy requirements. The use cases illustrate how manufacturers are addressing critical security and patient privacy issues.

Each organization using remote service will need to understand the requirements of applicable laws, and determine the security and privacy controls that are available in the remote service installation of any particular Medical IT System. Throughout this White Paper, the term "requirement" describes the high-level generic needs and obligations that might arise from national or regional legislation. However, the White Paper is not intended to be a comprehensive review of law or legislation. Instead, it focuses on the good-to-best-practice security and privacy controls that should reasonably be available in the healthcare IT-based systems. The White Paper provides examples of those instances when data privacy and security concerns might arise, and how manufacturers manage these concerns in order to help customers fulfill legal requirements.

This White Paper applies to all systems that have remote service capability and are part of healthcare delivery, e.g. HIS (Hospital Information Systems), PACS (Picture Archiving and Communication Systems), imaging systems, radiation therapy systems, and patient monitoring systems.

It is directed towards healthcare providers' IT professionals and assumes a basic understanding of IT infrastructure and security technologies. As always, for a full understanding of security and privacy controls on a particular system, the vendor remains the primary source of information.

2. Use cases

The careful application of remote service avoids time-consuming, on-site visits of service staff. The greatest customer benefit is realized when short-notice, critical service is necessary (or can be avoided). This section describes examples of typical time-critical use cases, and how remote services help minimize the system maintenance impact on the continuity of care.

2.1 On-demand services

2.1.1 Accidental data deletion

Patient data has been accidentally deleted. The recovery of deleted data, e.g., in a critical situation, has the greatest chance of success if the data is recovered immediately before any other system operations are performed. If the recovery process is unduly delayed, this data may be irretrievably lost as deleted regions of a storage device are reused and overwritten. A loss of this kind would require new manual input of data, or even the repetition of a medical procedure with all of its attendant medical risks for the patient.

2.1.2 Problems encountered during a medical procedure

Generally, technical questions or problems may arise at any time of day, and also during the performance of medical procedures. In these instances, the physician needs to decide as quickly as possible whether the medical procedure must be halted or if it may be continued after a brief equipment downtime. A remote service connection may allow a service organization to immediately assess whether a technical problem may be immediately solved or will require a longer downtime.

2.1.3 Restart after a system failure

A healthcare IT system failure often has severe consequences for the workflow at a healthcare delivery site, and typically requires restarting of the system. A restart, controlled and supervised by a technician, allows corrective actions to be performed remotely thus minimizing system downtime and providing some assurance of continued smooth operation. In such cases, remote service reduces local workflow disturbance, as well as avoiding the delays and costs of sending a technician to the customer site.

2.1.4 Support in case of shortage of resources

The continued operation of an IT system may be affected by shortages of equipment resources or staff. Each of these may impede the provision of care by disrupting local workflow.

- Shortage of equipment resources: An unexpected shortage of data storage space may prevent a system from further acquiring or processing data. A temporary electronic transfer of data to external third parties, until additional storage volume is made available, may help bridge such a shortage, and may shorten the interruption of the delivery of healthcare.
- Shortage of staff: Unscheduled staff shortages due for example to staff illness, can also hamper healthcare delivery. This negative effect may be reduced if the manufacturer is able to support local processes by controlling and executing some essential tasks from its remote service center (e.g., initiating backups or perhaps guiding local personnel).

2.1.5 Enhanced problem-specific monitoring

Some technical problems may appear and disappear sporadically, thus disrupting care and making problem diagnosis and resolution very difficult. Remote services permit the temporary use of specialty service tools that more precisely monitor the local system and can inform a service technician via network connection when the problem has reappeared. Some of these problems arise from network connection issues which may require the monitoring of network traffic during long periods of time (days or even weeks). Without remote services, the delays and costs for resolving these problems on-site could be very high. Other reasons for monitoring might include intermittent motor problems, temperature problems etc.

In the highly-interconnected IT environment of a modern healthcare provider, the identification of the specific system that causes a technical problem may be difficult. Sometimes several systems may contribute to creating the problem. A simultaneous and coordinated investigation by all involved manufacturers is required to isolate the cause(s) of the problem. Remote service permits the timely and cost-effective coordination of all parties needed to resolve these difficult problems.

2.1.6 Application support

The installation of a new system or application always involves a period where technical staff is learning how to best use the new features. Keeping this learning time short, and optimizing system use improves the quality of care. Remote service tools can allow system experts to coach technical staff during “look-over-the-shoulder” sessions. The sharing of screens and coach-trainee dialog can very quickly build expertise within the healthcare organization. Operational questions, problems or inefficiencies can be quickly resolved in a personal, supportive manner by leveraging remote service connection.

2.2 Routine services

The above use cases provide some clear examples of the benefits that accrue to healthcare providers through the careful application of remote service for Medical IT Systems. The quality of care delivered improves when providers are assured of a high level of system availability (uptime-rate) while protecting patient data. The benefits follow from:

- Increased system availability provides more time for medical diagnosis and treatment and avoids error-prone “work-arounds” required when critical systems are down. Fully operational systems enable medical staff to concentrate on delivering high-quality healthcare services to patients.
- Effective use of manufacturer service staff for remote access. Remote service tools allow the manufacturer to maintain a small staff in a few service centers around the world while carefully controlling and auditing their access. This provides security controls and minimizes the number of service engineers that need to have access to patient data. This limited group, plus the ability to monitor all of their access to healthcare provider systems, can provide a more controlled environment than on-site, on-call staff visits to the actual sites, thus helping mitigate security and privacy risks.

2.2.1 Software downloading and/or system upgrade and testing

System remote service connectivity offers an excellent opportunity to provide rapid system upgrading, patching, and other software modifications. This can be done as a pre-staged download prior to a customer service engineer arriving on-site, or it can be part of a remote upgrade session. When doing upgrades or system modifications remotely, the customer service center must carefully coordinate with clinical staff to take the system out of clinical service and define a way to restore clinical service after service operations are complete. Consistent with appropriate medical device regulations, the remote service center may need local

assistance to assure full post-upgrade verification on site. This sometimes requires facility technical staff to assist in carrying out pre-release testing.

2.2.2 System monitoring to avoid technical problems

Modern remote servicing entails the monitoring of system technical parameters during the routine operation of the IT systems without disturbing their medical use. Often this communication of status information is initiated from the medical system and communication via secured network proceeds to automatically transfer system condition information to a remote service center for inspection. Remote service staff do not actually log onto the healthcare organization's system unless an alert is sent from the system status analysis system. If a parameter, e.g., operating hours, available storage volume of an archive, etc., manifests values that may indicate possible or near-failure conditions, early countermeasures can be scheduled. Implementation of these countermeasures protects the healthcare provider from unscheduled and unexpected downtime and provides local flexibility and decision making to ensure the quality and continuity of healthcare.

3. Boundaries on remote service

3.1 International aspects

Medical device manufacturers operate globally. They are likely to have multiple remote service centers around the world providing first and second-level product support. Often, the third-level deep knowledge about a specific product is in a single manufacturing or research and development site. The tremendous advantage of real-time network-connected remote service is the speed with which a manufacturer's support organization can get answers from all three levels of expertise. This saves both cost and time. The technical experts required to solve a technical problem may be located on the other side of the globe. Today, it is unrealistic to expect that experts who are trained to address all technical problems are located in every country. Instead, they are distributed globally in a cost- and service-effective way to maximize the provision of needed services to the healthcare provider organizations.

3.2 Risks related to remote services

The benefits accrued by remote service do come with added risks for the security and privacy of data and systems. Security risks cover potential compromises to the confidentiality, integrity, or availability of data or systems. A privacy compromise often means a loss of control over personal information as a result of a security breach (loss of confidentiality). Some users may be concerned that remote access opens the door to potential, unauthorized access and damaging invasions of their Medical IT Systems.

In principle, unprotected or poorly configured network access to IT systems can give malicious individuals the possibility of attempting access without constraint and with very little risk on their part. Furthermore, vulnerabilities identified on one system can be reused on many systems of the same type. The potential system security compromises which may occur in remote service can be broadly classified in two problem sources:

- Unintentional actions caused by miscommunication between clinical staff and remote service experts, often as simple as misidentification of the system to be serviced (e.g., wrong network address). Such events are more likely to occur while remotely accessing systems rather than performing the services on location.
- Intentionally disruptive or furtive actions of malicious individuals using the network access to abuse the systems for their own purposes. Expert hackers, or even technically inclined

teenagers, are known to have accessed, used, or, through malicious software, caused damage to perceived secure systems.

The increased potential for unintentional or intentional wrongful actions should not be ignored, either by the manufacturer or by the user, when installing the IT infrastructure used for remote servicing. Because proper remote service crosses the boundary between the service delivery organization and the healthcare organization, security and privacy are joint responsibilities requiring a high level of cooperation and trust. Combining the fundamentals of the Hippocratic Oath with the role of the Medical IT System in the healthcare provider's mission, the SPC recognizes the three most essential properties of Medical IT Systems (in order of priority) as: (1) safety, (2) effectiveness, and (3) privacy. This guides our priorities in maintaining Medical IT Systems and helps us organize our action concerning threats to the delivery of care.

3.2.1 Threats to patient safety

Actions impacting patient and clinical staff safety are of the highest concern. They may be caused by movement of mechanical components, changes in machine operation (impacting x-ray dosage, energy delivery, etc.), interruption or early start of treatment, or changes in an individual's medical record. All could lead to significant safety risks for patients and medical staff.

3.2.2 Threats to effective care

As for any networked device, there are risks associated with the availability of systems and the data they contain. Direct malicious attacks on Medical IT Systems via viruses, Trojans, worm propagation, denial of service attacks, or system use to access yet other systems are amongst the most common compromises.

3.2.3 Threats to the protection of personal information (including medical privacy)

Payment information misuse, identification theft, disclosure of V.I.P. information, insurance fraud, loss of critical treatment information – all of these are potential threats associated with Medical IT System network connection. Although these events can be considered secondary when compared with patient safety and effectiveness of medical treatment, the impact of personal data disclosure can be severe to the patient as well as to the healthcare provider and equipment manufacturer.

This White Paper assumes that the Medical IT System has been developed according to medical device regulatory guidelines. Under these regulations, the means of providing service remotely should be engineered, designed, and tested for safety and effectiveness of the medical device. This would include technical, administrative, and physical controls to provide for safe and secure operation.

Where a Medical IT System has not been subject to medical device regulation, it is advised that the healthcare facility, in cooperation with the system manufacturer, develop a risk management plan that properly manages risks associated with safety, effectiveness, security (including privacy), interoperability, and other functional requirements.

As a help in managing these kinds of systems when they connect to networks (e.g., remote service), the standards community has organized a Joint Working Group 7 of ISO Technical Committee 215 and IEC 62A Subcommittee 62A to create a new standard, IEC 80001 "The application of risk management to IT networks incorporating medical devices". This standard will provide basic processes for the risk management of network connections of these systems. It is expected to become an official IEC standard in 2010.

4. Access to patient data

Remote access sessions can be categorized as to whether patient data are or can be accessed during a remote servicing session. This categorization is independent of the use cases referenced above and the technical capabilities of the system

4.1 Remote maintenance without access to patient data

In the case of automatic reporting of system condition, only system status information is transferred – for example the monitoring of system parameters to anticipate component problems or out-of-bounds operation that demands service attention. From a data privacy protection perspective, as well as a customer perspective, this is the ideal situation.

Some systems are designed to allow data anonymization before inspection by remote personnel. For example, the quality of a DICOM image can be investigated even if the accompanying patient-identifying information in the DICOM header is overwritten or erased before transmission. Such an anonymization function can be incorporated as an option in the Medical IT System prior to sending for problem diagnosis.

4.2 Access to patient data: potential or even required

When increased system expertise is required to diagnose and repair Medical IT Systems, access to all components and data within a Medical IT System may be required. It is less likely that patient data are accessed during the initial telephone service contact (called 1st tier service or the problem clarification stage) when information are gathered about “what happened”. However, once an equipment specialist (2nd tier), or even a factory-based engineer (3rd tier), is called in, it is much more likely that the in-depth investigation requires broad internal system access, including patient data access.

The normal in-depth access of 2nd and 3rd tier service via remote service has arisen because diagnosing equipment in this manner maximizes information to the service engineer and thus reduces servicing delays and costs. However, when servicing certain Medical IT Systems, the nature of the medical application may require that private information be transmitted to perform the service. For example, a PACS (Picture Archiving and Communication System) contains a database of image-related medical records. Depending on the configuration and the local use of the PACS, it may contain part of or even all data available about a patient, including administrative data as well as the full medical history. Because the PACS database (or any other database) can consist of comprehensive patient data, it is very likely that patient data will be accessed. In addition, the resolution of a problem using problem-specific monitoring files (see 2.1.5) may require exposure to patient data.

This limits the manufacturer’s ability to eliminate exposure to personal data by technical means. For those situations, non-technical administrative solutions must be defined and applied by both the healthcare provider and the remote service center. Appropriate policies will determine clear procedures, contractual terms, activity auditing, and other control measures. The implementation of such measures will protect the data accessed during a service session and will allow equipment repair to proceed effectively.

5. Technical and organizational solutions regarding remote service

Technical and organizational policies and procedures regarding Remote service can be least restrictive when there is no access to patient data while they have to be more stringent when patient data can be or are accessed during a remote service session. The organizational policies and procedures which are needed to manage information security require a certain amount of mutual trust and confidence that can be facilitated if the remote service center

operates in a manner consistent with established security controls such as those described by ISO 27001 "Information technology -- Security techniques -- Information security management systems – Requirements".

This section contains a collection of customer requests that are often encountered by the contributing companies and includes possible solutions implemented by the remote service organization. While they are very much the same as documented in the first SPC White Paper on remote servicing "Security and Privacy Requirements for Remote Servicing" (November 2001), additional customer security recommendations are included. This section concludes with Table 1 which delineates ownership of responsibilities for implementing the security controls to the manufacturer and to the customer respectively.

5.1 Organizational policies and procedures

Organizational policies and procedures define the umbrella under which remote services can be performed. There is a clear need for manufacturers as well as for customers to be able to rely on a globally harmonized set of policies.

As international regulations differ in many details, this White Paper cannot offer a complete and globally accepted set of policies but will instead describe the current set of organizational practices used to protect both the Medical IT Systems and the medical data accessed during a remote service session.

The goal is to deliver effective service at reasonable cost, while maintaining the security of the system and its data. It is presumed that organizational policies and procedures can be negotiated in detail, typically involving risk managers, privacy officers, and remote service center management as well as legal and regulatory staff.

Key elements of these organizational policies and procedures include:

- Provision that the remote service session is conducted from secure locations in accordance with applicable legislation where controls are in place to avoid unauthorized access that might occur by electronic or visual eavesdropping.
- Provision that service staff is bound by policy to keep information confidential (and trained to such policy).
- Directives that protected data (personal data, health information, etc.) are accessed and processed only in compliance with the contractual agreement.
- Explicit conditions defining who can obtain service activity audit records under which conditions and how long the manufacturer will retain them.
- Mechanisms for resolving connectivity problems between customer site and the manufacturer's remote service center.
- Regular monitoring of processes, controls and personal data related activities.
- Verification by each organization that it has met its own regulatory requirements prior to the initiation of remote service.

5.2 Technical Practices

5.2.1 Authorization to Connect

The connection to customer systems including possible access to patient data stored on those devices requires the active and informed customer consent in advance. This may include either:

- a long-standing authorization for continuous monitoring and/or for preventive maintenance of customer systems or

- short-term authorizations that may be required for a specific service episode.

The following items may be seen in service agreements:

- pre-determined timing for access to systems.
- periodic and off-peak access for preventive (predictive) maintenance.
- the ability for the customer to know (via visual cue) when remote service is active.
- the ability for the customer to reject and/or disconnect a service session.

5.2.2 Proper identification and authentication of the remote service center

The healthcare facility has a need-to-know requirement regarding individuals accessing its Medical IT Systems. Because service is a shared activity among a pool of highly trained individuals, this requirement can be met in a two-stage process. First, the manufacturer must have controls that limit access to the remote servicing center and restrict the ability to perform a service session to authorized and trained service staff. In a global, multi-device operation, the manufacturer controls will frequently limit access to a known, selected, qualified pool of engineers. The actual identity of the person performing service is managed and audited at the remote service center. Second, when a Medical IT System is connecting to a remote service facility, there must be a clear identification and authentication of the remote servicing center itself. Possible technical solutions to properly identify and authenticate a service center were published earlier in the SPC White Paper "Remote Service Interface – Solution A: IPsec over the Internet Using Digital Certificates" (Version 2, December 2003).

The above controls are intended to replace some customers request to individually identify service engineers on each system in the field. To allow such individual log-on requires complex functionalities of the system and would considerably raise the cost of service.

5.2.3 Audit trails

Service activities should be recorded at an appropriate level of detail. Usually this will be realized via automated audit records, but in specific situations a work report can also be appropriate. The records should serve to support after-the-fact investigations to verify whether unauthorized activities were started during a service session. They should help to detect instances where further analysis is required to increase the level of data security and data privacy. While the mechanism for recording service activities and the specific details recorded are left to the vendor, healthcare facilities should have the opportunity to review audit records upon request. The SPC recommends one year as an appropriate retention period.

Audit records should contain:

- date and time of the event (start/end).
- unique identifier sufficient to trace activity to the service engineer performing the actions.
- unique identifier of the system accessed.
- identification of operational and diagnostic activities performed (e.g. patch installed, configuration changed, image downloaded (de-identified or not), data base repair, what service tool was started).
- identification of files uploaded and/or downloaded (e.g., just the filename).

Audit records should not contain patient identifying information since the inclusion of personal information would then require additional protection and controls. The SPC also recommends against any kind of key stroke logging during a service session, as that is likely to contain personal data or ePHI.

There is often a perceived need to include operator information in audit records. It is important to realize that including operator names and times of operations constitutes personal data in some jurisdictions. There will be a need for additional protection and controls if records contain this personal data.

5.2.4 Secure and confidential (encrypted) transfer and storage of patient data

A principal requirement when performing remote service activities is to keep patient data confidential. There are well-established technologies that ensure confidential transfer of patient data (refer to SPC White Paper "Remote Service Interface – Solution A: IPSec over the Internet Using Digital Certificates" (Version 2, December 2003)). Today, other technologies such as, VPN, TLS, SSL, SSL-VPN are mature enough to safeguard the required level of data privacy and data security. Additionally, local regulations may influence the final choice of the encryption method or key length or even the use of encryption within the organization's network.

Any storage of personal data at the remote service center should be limited to only that necessary to resolve the particular service incident. Protective measures of remote service personal data storage should include enhanced security measures and consider full encryption of the data.

5.3 Recommended responsibilities when implementing remote services

This White Paper describes that secure remote service sessions require the fulfillment of responsibilities by both the healthcare organization and the service organization. Table 1 sets forth the respective responsibilities for the implementation of technical and organizational measures associated with remote servicing.

Table 1: Recommended Responsibilities for the Implementation of Technical and Organizational measures

Controls	Recommended Responsibility for Implementation	
	Healthcare Organization	Service Organization
Organizational policies and procedures (sec. 5.1)	Standard contract clauses offered by IT System Service Organization usually offer a high level of reliability.	Standard contract under applicable law should be used to avoid complicated management of individual clauses during or immediately in advance of a service session.
Authorization to Connect (sec. 5.2.1)	Service contract contains clauses about authorizations to connect.	Remote service center must be aware of customer-specific contract requirements (the use of standard contract clauses is strongly encouraged)

<p>Proper identification and authorization of the remote service center at the customer site (sec. 5.2.2)</p>	<p>Service contract requires that the service organization</p> <ul style="list-style-type: none"> - has a process to approve remote access authorization to trained and legitimate individuals - can trace all service activity back to an identified person. 	<p>Remote service center has technical and administrative controls to enforce identification and authorization of service staff, incl. auditing of their activities.</p>
<p>Audit trails (sec. 5.2.3)</p>	<p>Service contract requires service organization to retain audit records of sufficient detail to permit investigation. Audit of audit records permitted under contract.</p>	<p>Audit records collected and secured at remote service center should be retained for one year. Records are maintained in a manner that permits customer audit.</p>
<p>Secure (encrypted) transfer of patient data (sec. 5.2.4)</p>	<p>Service contract language restricts access to patient data as that data necessary for the resolution of a service issue.</p>	<p>Data transfer is recorded and data stored in a secure, possibly encrypted form. Technical and administrative controls exist to assure data destruction following closure of a service issue.</p>

6. Conclusion

Services to Medical IT Systems from remote service centers are now done every hour of every day around the world. The effective delivery of remote service can increase system availability and performance as well as provide savings in equipment maintenance costs. However, remote access capabilities come with the risk of unauthorized access and the dangers of system compromise and inappropriate disclosure of medical information. To ensure continuity of care, appropriate technical and organizational measures including contractual agreements must be in place.

Recent advances in technology allow for the remote servicing to Medical IT Systems in a secure and effective manner. The tools and connections used to provide these services require careful design as well as continuous monitoring and improvement to maintain the level of quality and security while dealing with emerging risks.

This White Paper details some of the practices in remote service. The complexity of networks and IT equipment requires that customers and manufacturers must clearly understand their responsibilities in this maintenance partnership.

One final cautionary note is in order. As a community, the SPC has focused on technical solutions that enable remote service and it is important that manufacturers continue to provide secure solutions for remote servicing of their systems.

However, ongoing efforts must also be made to keep abreast of laws and regulations, such as those intended to control the cross-border movement of information essential to effective servicing of Medical IT Systems. National and regional laws for the protection of personal data currently exist and continue to evolve. Although beyond the scope of this White Paper, it is essential that the medical device industry and the healthcare provider community work together to understand their impact on remote services.

Manufacturers must have security and privacy controls and need to clearly articulate the data flows in remote service. Customer organizations need to understand and meet their local data protection obligations. Both must work together to comply with regulations but must also

work with lawmakers and regulators to achieve practical protection for cost-effective equipment servicing and quality healthcare.