# Table of Contents

Overview ........................................................................................................... 3

Hijacking Life Support: Medical Device Risks ................................................ 4

The Weakest Link ............................................................................................ 4

Defining Medical Devices ................................................................................ 5

Breach and Patient Harm .................................................................................. 5

Patient Safety Implications .............................................................................. 6

Medical Device Security Regulatory and Standards Landscape .................... 6

Communication and Governance Challenges ................................................ 7

Technical Vulnerabilities .................................................................................. 8

Building a Robust Medical Device Security Program .................................... 10

Guidelines and Frameworks .......................................................................... 10

Assessments and Governance ....................................................................... 12

Communications .............................................................................................. 12

Asset Inventory and Scanning ......................................................................... 13

Virus/Malware Protection ................................................................................ 15

Patching ........................................................................................................... 15

Technical Security Controls ............................................................................ 15

Validation ......................................................................................................... 16

Training ............................................................................................................ 17

Network Isolation ............................................................................................. 18

Conclusion ........................................................................................................ 19
Overview

Medical devices include all those devices (hardware and software) used in patient care for diagnosis, treatment, and monitoring. This extends to ancillary support devices that are required for the medical device to function properly and are hosted on a clinical network such as external disk storage, database servers, and gateway or middleware interface devices.

Medical devices have historically had limited interoperability and communication capabilities and were not designed for the large-scale, integrated network environments of the modern healthcare ecosystem. Devices that once only transmitted data to a display in the patient’s room are now transmitting patient data to Electronic Health Records (EHRs), nursing stations and physician tablets by way of monitoring devices, pumps, ventilators, imaging systems, and other point of care devices.

The lack of historical focus on building security requirements into medical devices has led to these devices becoming one of the weakest links in the chain for securing healthcare networks and systems. Medical devices have become a gateway to a healthcare organization’s domain, opening the door to a trove of patient health information and regulated data.

Security incidents related to medical devices also have the potential to impact patient safety and do meaningful harm to patients connected to these networked devices. This report outlines the risks and impacts associated with medical device security and also provides leading practices for developing medical device security programs.
Hijacking Life Support: Medical Device Risks

The Weakest Link

Healthcare providers rely on medical devices to sustain high quality patient care, however, the vulnerabilities in these devices could put patients and their information at greater risk. Devices that are directly connected to patients can be reconfigured by malicious attackers to deliver lethal dosages of medications, prevent life-saving alerts, or rendered completely useless.

Healthcare organizations have also become a favored target of cybercriminals due to the weak security protections found standard among most medical devices and their ability to serve as an access point to sensitive healthcare data.

Health information, such as that found in medical records, does not change even if compromised. As such, this information can be used to commit multiple types of fraud (including identity theft) and takes twice as long to identify compared to identity theft that does not utilize health information. This advantage makes health information significantly more valuable to cybercriminals than other personal data such as financial information (banking account or credit card numbers) and is 50 times more valuable than a stolen social security number.¹

![Figure 2: An example of a networked life support device](image)

Medical devices have become one of the weakest links in the security protection of healthcare providers for reasons including:

- Medical devices are increasingly network connected
- Healthcare data is increasing in value for cyber criminals
- Default passwords, missing patches, remote access, and other weaknesses make medical devices a prime target for entry
- Incidents with medical devices can impact patient safety and can also lead to data breach and regulatory action

Defining Medical Devices

While there is no universal definition of a medical device, the Department of Veteran’s Affairs (VA) defines it as any component(s) [hardware, software] that is/are:

- FDA 510K certified
- Any device that is used in patient healthcare for diagnosis, treatment or monitoring
- Any ancillary support device (e.g., external disk storage, database servers, gateway or middleware interface devices) required for the medical device to function properly²

The table below identifies medical device categories as well as examples of medical devices.

<table>
<thead>
<tr>
<th>Device Category</th>
<th>Example Devices and Uses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Cardiac (EKG, Holter, Swan-Ganz), hemodynamic (blood pressure cuff, arterial transducer), respiratory (pulse oximetry, capnography, thoracic transducer belt), neurological (intracranial pressure, electroencephalography, bispectral index), blood glucose, childbirth, body temperature</td>
</tr>
<tr>
<td>Diagnostic</td>
<td>Ultrasound, Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET), Computed Tomography (CT), x-ray</td>
</tr>
<tr>
<td>Treatment</td>
<td>Infusion pump, LASIK, robotic surgical system, cardiac catheterization lab, linear accelerators (LINAC)</td>
</tr>
<tr>
<td>Therapeutic</td>
<td>Continuous Passive range of Motion (CPM) machines, communication and cognitive devices for physical, sensory and cognitive disabilities</td>
</tr>
<tr>
<td>Analytical</td>
<td>Blood Gas analyzer, cell counters, coagulation analyzer, electrolyte analyzer</td>
</tr>
<tr>
<td>Life Sustaining</td>
<td>ventilators, defibrillators, anesthesia delivery systems, cardiopulmonary bypass machines, Extracorporeal Membrane Oxygenation (ECMO), dialysis</td>
</tr>
</tbody>
</table>

Breach and Patient Harm

There are indicators that the health care industry lags significantly behind other regulated industries in securing and protecting sensitive information. Healthcare is 30% more likely than the financial industry to have sensitive assets stolen, 17% more likely to experience a security incident related to employee errors, and 20% more likely to experience an incident related to the misuse of privileged access.³ This state of affairs creates an increased likelihood that medical device security may continue to lack effective security for some time to come.

---
In addition to physical harm, many networked medical devices can be a gateway to a healthcare organization’s domain, opening the door to a trove of protected health information. Medical information is valued at an all-time high on the black market, making medical devices a prime target for hackers and thieves. 

A breach of a healthcare organization’s information security can result in patient harm, financial loss, and damage to data and reputation. Often, it is all the above. Medical identity theft affected an estimated 1.5 million people in the U.S. at a cost of $41.3 billion last year. The dominant method of breaching healthcare security in 2015 was hacking.

**Patient Safety Implications**

The compromise of medical devices by malicious actors or software can impact a great deal more than patient privacy, patient data breach, or potential financial and reputational damage. Devices that malfunction due to unauthorized access or activities has the potential to directly impact patient safety and the quality of care. Some examples of patient safety implications for medical devices include:

- Security researchers demonstrated that it was possible to hack a pacemaker remotely and cause it to deliver a life-threatening jolt
- Wireless attacks have been conducted on insulin pumps, patient monitors, infusion pumps, and imaging devices
- Loss, corruption, and interception of data can cause severe impact to patient health and safety
- Attacks are often indiscriminant malware that target unpatched systems including medical devices

**Medical Device Security Regulatory and Standards Landscape**

Medical device security standards and regulations have received increased attention and development over the last several years from a host of federal and private sources. However, guidance from the federal government via the FDA and other sources listed in the figure below has lacked formal mandate authority. Such guidance is also missing prescriptive details the industry needs to implement effective medical device security programs. Relevant regulations and standards have to date not carried along meaningful incentives or disincentives for providers like to invest time, resources, and energy to tackle this problem.

---

Private industry consortiums have cropped up and are helping to provide more prescriptive guidance, but there remains to be a clear and concise framework or standard that is comprehensive and prescriptive enough to tackle the challenge. The result is a hodge-podge of guidance, frameworks, and tools that lacks cohesion.

Communication and Governance Challenges

The level of awareness of medical device security challenges has risen significantly in recent years, however, a general lack of coordination across industry segments and stakeholders has impeded progress for providers. Clinical Engineering and IT departments have historically been separate business units and often did not include security oversight of medical devices.
Technical Vulnerabilities

There are a host of challenges involved in securing the infrastructure of a healthcare organization. Many of these are exacerbated by the lack of industry awareness of known vulnerabilities and vulnerability and patch management rigor is often not applied to medical devices. Furthermore, medical devices may run on legacy operating systems that are no longer supported by original manufacturers. Once the device has outlived its support timeframe, manufacturers often may not create or release security patches or software updates to these devices. Moreover, when it comes to patching these devices, most healthcare organizations are uncertain as to who is responsible for ensuring that these devices stay up to date with the latest patches. Responsibilities for patching devices with the latest software and/or firmware is unclear and not formally defined.

Although there are some federal regulations and guidance put in place to improve the quality and function of devices, these requirements can also unintentionally inhibit the securing of these devices. There remains a perception by some in the industry that FDA and other regulations prohibit the routine updating and patching of security vulnerabilities for medical devices. However, the FDA has gone on record to clarify that patching of known security vulnerabilities is both appropriate and required. A lack of clarity in responsibility (e.g., who is held accountable for patching) in an organization can also be considered a challenge.

The figure below identifies some of the most common security vulnerabilities found in medical devices.

Figure 5: Medical Device Security Vulnerabilities

Vulnerability Management

- Overly broad anti-virus exceptions (e.g. providers instructed not to scan the C: drive of the medical device or server)
- Lack of sharing of medical device vulnerabilities across customers (NDAs and other contracts limit information sharing including vulnerabilities)
- Lack of network segmentation to isolate medical devices from other unrelated critical systems
- Cybersecurity vulnerability research is often viewed as disruptive
Reliance on Third-Parties

- Dependence on third parties to manage and secure devices
- Vendor access and updates often occur outside of standard access control and change management processes
- Medical device security is not always considered during procurement processes and purchasing decisions
- Security is often not considered in the software development life cycle for medical devices
- Lack of accountability for implementing security controls
- Default vendor accounts
- Inconsistent and insecure technical security controls
  - Weak password management controls
  - PHI not encrypted or weak encryption enabled
  - Weak wireless encryption

Fragility

- Fragile legacy devices and platforms inhibits patching activities
- Hesitancy from IT security operations in scanning medical devices, due to fears of “bricking”, blue screening or otherwise making a device unusable after a vulnerability scan

Inventory Management Woes

- Medical device inventories are incomplete, inaccurate or are missing necessary information
- Traditional network scanning and discovery tools are not always equipped to scan and identify medical devices specifically, and such scans may themselves adversely impact medical devices
Building a Robust Medical Device Security Program

Due to the extensive amount of vulnerabilities to information security that necessary medical devices present to healthcare organizations, a robust Medical Device Security Program (MDSP) should be established and maintained to prevent costly information breaches. This section provides guidance on industry leading practices for developing and maintaining medical device security programs.

An MDSP should be designed to be a repeatable and prescriptive model for healthcare providers to assess, implement, and communicate security risks associated with medical devices. The program brings together key stakeholders including Clinical Engineering / Biomedical, IT, security and compliance, legal, training, and purchasing departments to address the unique challenges presented by medical devices.

Guidelines and Frameworks

Several government and industry entities have provided standards for securing medical devices. Although these are not legally enforceable, Meditology recommends suggested that healthcare organizations align with one or more of the frameworks proposed by our organization, the VA, FDA, International Organization of Standardization (ISO), the Medical Device Innovation, Safety, and Security Consortium (MDISS), and Healthcare Information and Management Systems Society (HIMSS).

Recommended Frameworks

This list is not exhaustive, but rather represents several of the frameworks and standards that Meditology recommends providers consider in the development of the MDSP.
U.S. Department of Veterans Affairs Medical Device Protection Program (VA MDPP)  

The VA has developed the Medical Device Protection Program (MDPP). Once a component(s) [hardware, software] is categorized as a medical device, as per the VA’s definition of a medical device, it is subject to the MDPP. This program consists of seven parts:

- Communication
- Training
- Validation
- Scanning
- Remediation
- Patching
- Medical Device Isolation Architecture (MDIA)

Food and Drug Administration (FDA)  

The FDA has also developed guidance that is specifically targeted towards protection that can be implemented on existing devices as well as security considerations for the future design of medical devices. The FDA clearly establishes that the responsibility of securing medical devices lies with all stakeholders, not just vendors or end users. The core functions of the guidance include: the identification and protection of medical devices, limiting access to trusted users only, ensuring that content is trusted, detection, response, and recovery.

International Organization for Standardization (ISO)  

ISO 80001 is a congruent set of requirements developed by an international working group with members from the medical device industry, hospital Clinical Engineering, and IT. ISO 800001 is a systematic guide to help in the application of risk management when creating or changing a medical device IT network. It provides easy to apply steps, examples, and information helping in the identification and control of risks while remaining agnostic as to the underlying controls framework.

Medical Device Innovation, Safety, and Security Consortium (MDISS)  

MDISS is an industry standards organization “focused on optimizing the relationship between the quality of health care and the process of assessing and ensuring that devices and systems are secure and functioning in a safe and efficacious manner.” The organization includes membership from stakeholders including providers, device manufacturers, researchers, and other interested parties. MDISS issues guidance to the industry on securing medical devices and associated platforms.

Healthcare Information and Management Systems Society (HIMSS)  

Manufacturer Disclosure Statement for MDS2 is a tool provided by HIMSS. This form provides medical device manufacturers with a means for disclosing to healthcare providers the security related features

---

8 MDISS - http://www.mdiss.org/Home/About
of the medical devices that they manufacture. Key benefits of using the standardized MDS2 form include providing a comprehensive set of medical device security questions developed through broad stakeholder participation and medical device vendor buy-in, allowing for easy comparison of security features across different devices and different manufacturers, facilitating the review of the large volume of security-related information supplied by the manufacturers. (Ibid., ISO/TR 80001-2-6:2014)

Assessments and Governance

Organizations should conduct routine assessments of the maturity of their existing medical device security program, if one is already in place, to determine which areas need attention. Some of the activities involved in remedying weaknesses include the following:

- Conduct penetration testing/ethical hacking targeted at medical devices to identify actual weaknesses in the environment
- Create or update policies that define medical devices
- Ensure Biomedical/Clinical Engineering policies have been reviewed and/or updated by the Information Security group
- Create governance model and ensure that the Biomedical/Clinical Engineering group has a place in Information Security committees
- Establish formal communication and reporting channels between Biomedical/Clinical Engineering and IT departments
- Update training and awareness materials to include medical device security considerations
- Conduct targeted security awareness training for the stakeholders including the Biomedical/Clinical Engineering team(s)

Communications

The range and variance of stakeholders involved in securing medical devices creates a unique challenge for consistently applying security controls to these systems and devices. Continual coordination is necessary between all stakeholder groups including Information Security, Compliance, Privacy, Clinical Engineering / Biomedical, organizational leadership, IT, industry groups, medical device vendors, regulators, and others.
Formal structures and mechanisms should be created to maintain communication between various groups responsible for medical device security including:

- Leadership reporting
- Policies and procedures
- Governance committees
- Resource allocation and reporting structures

**Asset Inventory and Scanning**

**Asset Inventory**

Maintaining a current medical device inventory is vital to the success of the MDSP. The inventory defines the scope of medical devices in the program. The inventory data may be collected manually or by using discovery scanning technology.

Radio Frequency Identification (RFID) technology allows the tracking and tagging of medical devices via specialized software that can identify where devices are located at any given time. This technology should be explored to assist with the automation and accuracy of asset inventories as defined above.
Medical Device Classifications and Priorities

Providers should assign classification and priorities to medical devices based on the risk/type of device. The classifications may vary based on organizational priorities but could follow a model similar to the example described below.

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lifesaving (defibrillator, pacemaker, ventilator)</td>
</tr>
<tr>
<td>2</td>
<td>Curative/Therapeutic (infusion pump, hyperbaric chamber, dialysis)</td>
</tr>
<tr>
<td>3</td>
<td>Patient Diagnostic (ECG, Ultrasound, X-Ray, lab equipment)</td>
</tr>
<tr>
<td>4</td>
<td>Analytics (fetal monitors, patient monitors)</td>
</tr>
<tr>
<td>5</td>
<td>Miscellaneous (medical cabinet, autoclave, scale)</td>
</tr>
</tbody>
</table>

Security Classification | Description
--- | ---
A | Over 100,000 records stored, transmitted or processed
B | Between 10,001 and 99,999 records stored, transmitted or processed
C | Less than 10,000 records stored, transmitted or processed
D | Device does not store, transmit or process PHI

Vulnerability Scanning

If devices have never been scanned before, it is best to proceed cautiously until observations can be made on how devices react to vulnerability scanning. Older network equipment and devices may be susceptible to interference from scans and should be scanned using limited scan configurations. Some potential scan limitations can include:

- Scan devices on a separate network before they are put into productive use
- Scanning a single device before scanning an entire network range containing those devices
- Adjust scanning configuration settings to a limited number of plugins or scan types (e.g. disable Denial of Service, brute force, simultaneous TCP sessions, and other such settings)
- Enable safe checks if available in the vulnerability scanning tool

Prioritize scanning according to a classification scheme. An example scanning timetable is provided below.

<table>
<thead>
<tr>
<th>Medical Device Priority</th>
<th>Medical Device Classification</th>
<th>Quarterly</th>
<th>Bi-Annually</th>
<th>Annually</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>B</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>C</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>A</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>B</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>C</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>B</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>3</td>
<td>C</td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Virus/Malware Protection

Anti-virus and anti-malware protection may vary depending on the specific manufacturer line of device or type of device. The two primary deployment models are:

- Anti-virus solutions provided by the provider
- Anti-virus solutions by the medical device vendor

A separate and distinct process should be created for each of the scenarios above including considerations for installation, monitoring and alerting of incidents, exceptions tracking for devices that cannot meet the organization’s standards, and incident response and communication procedures.

Patching

Software and firmware patching processes for medical devices will be heavily dependent upon the device owner. Often, organizations will only keep devices until the vendor(s) discontinue support in the form of software updates or patches. Organizations will then purchase a new device, renewing the vendor support period. Sometimes however, there is a business need to keep devices long past the vendor support period.

The following are potential patch management approaches:

- Provider-managed devices – no vendor support
- Vendor only – vendors are charged with all updates and support to the device with no involvement from the provider’s staff
- Vendor provided and the provider installs – this may include patches that are provided via portal download and pushed by a local server or the delivery of a USB device
- Unsupported devices – devices that are not capable of receiving updates

Organizations should also define the tools, processes, procedures, and roles and responsibilities for patching. These requirements should be defined in a security standard and included in contracts and Service Level Agreements (SLAs) with vendors.

Technical Security Controls

Technical configuration and security controls should be implemented and enforced when using medical devices to protect information on the devices as well as the supporting IT infrastructure.

Examples of related technical security control activities include:

- Change or disable default vendor login accounts and passwords
- Segment medical devices from the rest of the network and limit to minimum necessary traffic, this protects the devices and protects other critical systems from damage from infected medical devices
- Ensure internet-facing systems are incorporated into a demilitarized zone (DMZ) model
- Require multi-factor authentication for remote access to medical devices
- Ensure IDS/IPS capability is in place for network segments containing medical devices
- Incorporate medical devices into audit log aggregation and monitoring solutions to gain visibility into suspicious activity on these devices
- Implement restrictions on USB functionality to limit malware infection and data loss exposures
Validation

As healthcare organizations work to improve their own practices and procedures as they relate to medical devices, they must ensure that the vendors that have access to their data environments are doing the same.

The goal of the validation stage is to identify variances in designed security controls in medical devices and the environments in which those systems operate. Partial or complete failure of deployed security controls, or the absence of controls, represents potential vulnerabilities that can be exploited by threat sources. Validation activities including risk assessments help determine the severity of such vulnerabilities which in turn can guide and inform organizational risk responses (e.g., prioritizing risk response activities, establishing milestones for corrective actions).

The success of the vendor validation process is contingent upon the following factors:

<table>
<thead>
<tr>
<th>Success Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Objectives</td>
<td>Clearly established goals and objectives for the medical device security assessment program</td>
</tr>
<tr>
<td>Leadership Reporting</td>
<td>Consistent communication plan/process to inform leadership of medical device vendor risk exposure</td>
</tr>
<tr>
<td>Negotiation Objectives</td>
<td>Clearly defined outcomes and options</td>
</tr>
<tr>
<td>Vendor Communication</td>
<td>Processes for the consistent and clear communication of expectations</td>
</tr>
<tr>
<td>Stakeholder Collaboration</td>
<td>Communication among key stakeholders to provide insight into current and upcoming vendor products, risk exposure, and scheduled audits</td>
</tr>
<tr>
<td>Risk Model</td>
<td>Model to consistently assess, prioritize and measure medical device vendor and product risk</td>
</tr>
</tbody>
</table>
The medical device vendor security validation process is further supported by the following activities:

- Inventory vendors and associated risk information
- Calculate risk for vendors
- Request a completed HIMSS MDS2 medical device security form
- Send out questionnaires or risk assessments to vendors
- Gather and evaluate vendor responses
- Track the status of vendor commitments
- Provide workflow capabilities to route documents for review and approval
- Archive documents/evidence of reasonable assurance obtained from vendors
- Report out metrics, status of risk management activities and executive level dashboards
- Leverage third party risk management firms like CORL Technologies (information available at [http://www.vendorsecurityrm.com/](http://www.vendorsecurityrm.com/)) to vet and maintain accountability of medical device vendors and products

### Training

The medical device security training and education approach helps to bridge the knowledge gap between disparate stakeholder groups responsible for securing medical devices and platforms.

In order for this program to be successful, all entities must have an understanding of each other as a whole. If units are created and then compartmentalized with little to no communication, decisions made in individual units will not have the input or oversight from the others, impeding the effectiveness of the program.

Training should be tailored to each stakeholder group and include some of the following considerations at a minimum:

- MDSP overview and roles and responsibilities
- Definition of medical devices
- Patient safety implications of medical devices
- Applicable regulations and standards
- Common security challenges with medical devices
- Examples and case studies of medical device security incidents
- Remote access standards and requirements
- Third party medical device vendor technical and security validation
- General device functions and cyber communication
- Awareness of operational policies and procedures
- Security incident response procedures (using medical device examples)
- Communication expectations

### Tools

<table>
<thead>
<tr>
<th>Tools</th>
<th>Tools to support data gathering, analysis, reporting and process workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Clear accountability and responsibility for vendor security risk management</td>
</tr>
<tr>
<td>Timing</td>
<td>Medical device vendors should be assessed for security controls prior to purchase to increase leverage on the vendor to remediate identified risks</td>
</tr>
</tbody>
</table>
**Network Isolation**

Network isolation involves the grouping of medical devices into protected network segments to limit the potential for unauthorized access or impact to the functioning of these critical pieces of equipment.

Network isolation helps to protect medical devices from threats on the internal provider’s network which may include viruses, malware, or other malicious attacks. Isolation also helps protect other critical assets from medical devices that may become infected with malware or accessed in an unauthorized manner due to relatively insecure configurations that have been documented throughout this strategic plan document.

Isolation also supports the ability for provider organizations to apply protection mechanisms specific to medical devices which may include specialized vulnerability scanning, increased network monitoring and alerting for medical device networks, more granular access controls, and other technical security mechanisms.

The specific network configuration and design of medical device networks and sub networks will depend upon multiple factors including the current state configurations of the provider’s internal network and networking capabilities.
Conclusion

Medical devices have become one of the weakest links in the security chain for healthcare entities over the past several years. Security incidents related to medical devices have the potential to negatively impact the safety of patients connected to networked devices, an organization’s reputation, and cause financial harm via costs associated with breaches and regulatory action.

Addressing medical device security requires consistent effort and communication across a myriad of stakeholders, both internal and external to provider organizations. The development of a formalized medical device security program that includes people, processes, and technology considerations is essential to ensuring the protection of medical devices and the patients they support.

About Meditology

Meditology Services LLC is a healthcare-focused advisory services firm with core principles of quality, integrity, loyalty, and value. We provide a range of healthcare security and privacy services from assessments, ethical hacking, staff augmentation, HITRUST and SOC 2 certification, and other compliance and risk management support. Our executive team has an average of 15 years of consulting and operational experience serving healthcare clients of varying size and complexity. We understand the importance of relationships and derive much of our business from a long list of satisfied clients who value the quality of our work products as well as the professionalism, approach, and innovative solutions we bring to our engagements.

For More Information

Meditology Services LLC
5256 Peachtree Road, Suite 190
Atlanta, GA 30341
info@MeditologyServices.com
Tel. (404) 382-7591
www.meditologyservices.com