

GUIDELINE OPEN ACCESS

Expert Consensus-Based Technical Guidelines for Remote Robotic-Assisted Surgery and Procedures

Yulun Wang¹ | Martin Buehler² | Shane Farritor^{3,4} | Yuman Fong⁵ | Mike Kijewski⁶ | Brian Miller⁷ | Bill Peine⁸ | Blair Whitney¹ | Mike Yramategui⁷ | Jordana Bernard¹

¹Sovato, Santa Barbara, California, USA | ²Johnson & Johnson, Santa Clara, California, USA | ³Virtual Incision, Lincoln, Nebraska, USA | ⁴Mechanical and Materials Engineering, College of Engineering, University of Nebraska, Lincoln, Nebraska, USA | ⁵Department of Surgery, City of Hope, Duarte, California, USA | ⁶MedCrypt, Solana Beach, California, USA | ⁷Intuitive Surgical, Sunnyvale, California, USA | ⁸Medtronic, Ashland, Massachusetts, USA

Correspondence: Jordana Bernard (jbernard@sovato.com)

Received: 30 May 2025 | **Accepted:** 31 May 2025

Funding: The authors received no specific funding for this work.

Keywords: healthcare telecommunications | latency | network structure | remote robotic procedure | remote robotic surgery | remote surgery | telerobotics | telepresence | telesurgery

ABSTRACT

Remote robotic-assisted surgery and procedures offer significant potential to enhance access to surgical expertise, optimize patient outcomes, improve healthcare efficiency, reduce costs, and increase patient and provider satisfaction, aligning with the quintuple aim. By mitigating geographic barriers, addressing surgical deserts, and reducing travel burdens for surgeons, patients, and their families, remote robotic-assisted surgery and procedures can substantially expand access to high-quality health care. The safe and effective implementation of remote procedures depends on the availability of robust, surgical-grade networks, reliable connectivity, and comprehensive cybersecurity measures to protect patient data. Seamless integration among remote-enabled robotic system interfaces, telepresence technologies, and facility-level infrastructure is essential to ensure operational reliability and procedural success. These technical guidelines define the fundamental technical requirements to support the design, implementation, and scaling of safe, effective, and interoperable remote robotic-assisted surgical and procedural programs. As the field evolves, guidelines will be updated to reflect technological advancements, specifications, and emerging best practices. Complementary clinical and operational practice guidelines will work synergistically with technical guidelines to support the global expansion and market adoption of remote programs.

1 | Introduction

1.1 | The Challenge of Surgical and Procedural Access

Access to surgical care remains one of the most pressing yet unsolved public health challenges. Surgical deserts—regions lacking adequate access to surgical care—are a well-documented global issue that affects both developed and developing countries. Today, over half of the global population

lives without sufficient surgical access [1]. Even in the most advanced healthcare systems and affluent countries, access to high-quality surgical care remains deeply inequitable, with approximately 24% of the population in high-income countries lacking adequate surgical access [2].

In the United States, a country viewed as a leader in healthcare innovation, over one-third of counties lack access to a single surgeon. This crisis is projected to worsen with an estimated shortage of up to 30,200 surgeons across all specialties by 2034 [3].

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2025 The Author(s). *World Journal of Surgery* published by John Wiley & Sons Ltd on behalf of International Society of Surgery/Société Internationale de Chirurgie (ISS/SIC).

Although surgical expertise is often concentrated in urban centers, patients in both rural and remote areas face overwhelming barriers to care.

Multiple factors, including a shortage of skilled surgeons and interventionalists, geographic barriers, rising healthcare costs, and financial pressures on healthcare providers, drive limited access to quality surgical care. The implications of inadequate surgical access are far-reaching: patients are left with limited, or often, no options for essential procedures, leading to costly and time-consuming travel, delayed care, or substandard surgeries and postoperative treatment. In the developed world, these barriers drive surgical delays, create capacity bottlenecks at high-volume hospitals, and force patients to travel long distances. In developing countries, the challenges are even more pronounced—many regions lack even the most basic surgical infrastructure.

1.2 | Impact of Remote Procedures

REMOTE ROBOTIC-ASSISTED SURGERY AND PROCEDURES (“Remote Procedures”) represent one of the most promising advancements in modern medicine. By enabling a surgeon to operate on a patient from virtually anywhere via a REMOTE-ENABLED ROBOTIC SYSTEM and high-speed network, remote procedures have the potential to redefine surgical access by erasing geographic barriers and increasing surgical efficiencies worldwide.

Although this concept is novel in its modern implementation, its foundations are not new. In 2001, the groundbreaking Lindbergh Operation demonstrated feasibility and safety with a transatlantic remote procedure [4]. In this surgery, surgeons located in New York performed a remote robot-assisted laparoscopic cholecystectomy on a 68-year-old woman in Strasbourg. The operation was successfully carried out across more than 14,000 km using a dedicated fiber-optic communications network between the sites. Subsequently, in 2003, surgeons in Ontario, Canada, performed 22 remote robot-assisted laparoscopic procedures between St. Joseph’s Healthcare Hamilton, a teaching hospital affiliated with McMaster University, and North Bay General Hospital, a community hospital located 400 km away. These operations were facilitated using an Internet protocol virtual private network [5]. Despite these early successes, further projects were abandoned in the mid-2000s due to high network costs, LATENCY challenges, a lack of societal readiness, and the halted development of remote-enabled surgical robotics. Over the past 2 decades, significant advancements in robotic-assisted technology, telemedicine, and telecommunications, particularly the expansion of high-speed, lower-cost networks, and reduced LATENCY, have reignited the potential of remote procedures as a scalable model of care [6–8].

Telemedicine has become a standard component of healthcare delivery and is typically used for consultations, even when the patient is close to their provider, as it is an effective delivery modality for both the provider and the patient. This serves as a model for remote surgery and procedures, demonstrating that

geographical distance, both near and far, should not be a barrier to accessing surgical expertise.

In developed countries, remote procedures will help alleviate the growing surgeon and workforce shortage, strengthen regional hospital networks, alleviate financial strain, and create access to care for underserved communities. Remote procedures will also contribute to broader healthcare objectives, including progress toward the Quintuple Aim—a framework guiding healthcare transformation through five key pillars: (1) improved patient experience, (2) better outcomes, (3) cost efficiency, (4) clinician well-being, and (5) health equity [9]. Remote procedure programs will drive efficiency by increasing a physician’s surgical capacity, optimizing operating room utilization through load balancing, and bringing the skills of specialists to where they are needed most. For example, enabling specialists to provide remote procedures across a healthcare system or group of hospitals will help small and mid-sized hospitals stay viable, expand patient choice, and lower costs. Beyond expanding access, remote procedures foster global collaboration, enabling physicians to share expertise, mentor colleagues, and provide advanced hands-on surgical training.

The ripple effect in developing nations will be profound. By setting a global precedent for safe, effective, and scalable remote procedures, this innovation paves the way for expansion into underresourced regions, delivering world-class expertise to areas where surgical care is otherwise lacking and/or nonexistent. Furthermore, following global efforts to enhance healthcare safety through technology, the World Health Organization’s Global Plan of Action for Patient Safety 2021–2030 explicitly recommends investing in the digitization of end-user health care services, such as telemedicine and teliagnosis, as a key strategy to reduce preventable harm and promote safer care delivery systems [10].

1.3 | Value of Industry Guidelines

As healthcare rapidly embraces this transformative technology, establishing comprehensive technical guidelines is critical to ensuring patient safety and maintaining universal quality. Recognizing this need, a working group of industry leaders was formed to develop technical guidelines to inform the design and implementation of REMOTE-ENABLED ROBOTIC SYSTEMS. This initiative followed industry-recognized guidelines development processes, including consensus-driven collaboration, broad stakeholder engagement with technical and clinical subject matter experts, and an extensive literature review.

Although primarily technical in scope, these guidelines have far-reaching implications for the entire remote procedures ecosystem, including patient care, operational workflows, and industry alignment. By establishing clear technical guidelines, this initiative aims to support the safe and effective expansion of remote procedure programs, providing a structured framework that plays a crucial role in shaping the future of surgical care worldwide. The ultimate goal is to democratize worldwide access to safe, high-quality, interoperable, and scalable surgical and procedural care.

1.4 | Applying the Guidelines

The resulting *Remote Robotic-Assisted Surgery and Procedures Technical Guidelines* define critical requirements for SURGICAL-GRADE NETWORK characteristics, cybersecurity, system interfaces, TELEPRESENCE, and facility-level considerations. The document also outlines additional key design and implementation requirements for REMOTE-ENABLED ROBOTIC SYSTEMS as well as cybersecurity best practices. These guidelines do not define specifications (e.g., NETWORK LATENCY, JITTER, and BANDWIDTH allocation) as these parameters vary based on the USE CASE and other factors. Additionally, these specifications will be validated through the development process for defined use cases.

As remote procedures continue to evolve, these guidelines will be updated accordingly to reflect technological advancements and emerging best practices. In addition, a range of clinical, operational, and ethical considerations must be addressed to ensure patient safety and support the broader adoption of remote procedures. Complementary practice guidelines, covering issues, such as liability, licensure, credentialing, and safety protocols, will align with the technical guidelines, working together to support the safe and effective expansion of remote programs [11–13].

1.5 | Intended Audience

These *Technical Guidelines* are intended for all stakeholders involved in designing, developing, or implementing REMOTE-ENABLED ROBOTIC SYSTEMS, including the following groups:

- Medical device manufacturers and robotic companies

- Telecommunications and infrastructure providers
- Technology and cybersecurity professionals
- Healthcare organizations, hospital administrators, IT, and other professionals
- Healthcare providers and clinical teams
- Research and academic institutions
- Healthcare regulators

2 | Scope

The *Expert Consensus-Based Technical Guidelines for Remote Surgery and Procedures* provide a framework of fundamental technical requirements to support the design and implementation of safe, effective, interoperable, and scalable REMOTE-ENABLED ROBOTIC SYSTEMS. These guidelines require collaboration among ecosystem stakeholders and should be considered in combination with other factors that contribute to safety that are beyond the scope of these guidelines.

The technical guidelines address these key components specific to remote procedures (e.g., robotic-assisted surgery [RAS] and interventional delivery systems) as shown in Figure 1:

1. Operational requirements for THE SURGICAL-GRADE NETWORK.
2. Cybersecurity requirements for the SURGICAL-GRADE NETWORK and REMOTE-ENABLED ROBOTIC SYSTEMS.
3. Requirements for system interfaces to operate over the SURGICAL-GRADE NETWORK.
4. Requirements for TELEPRESENCE in the REMOTE PHYSICIAN site and the PATIENT SITE procedure room.

Technical Guidelines Components

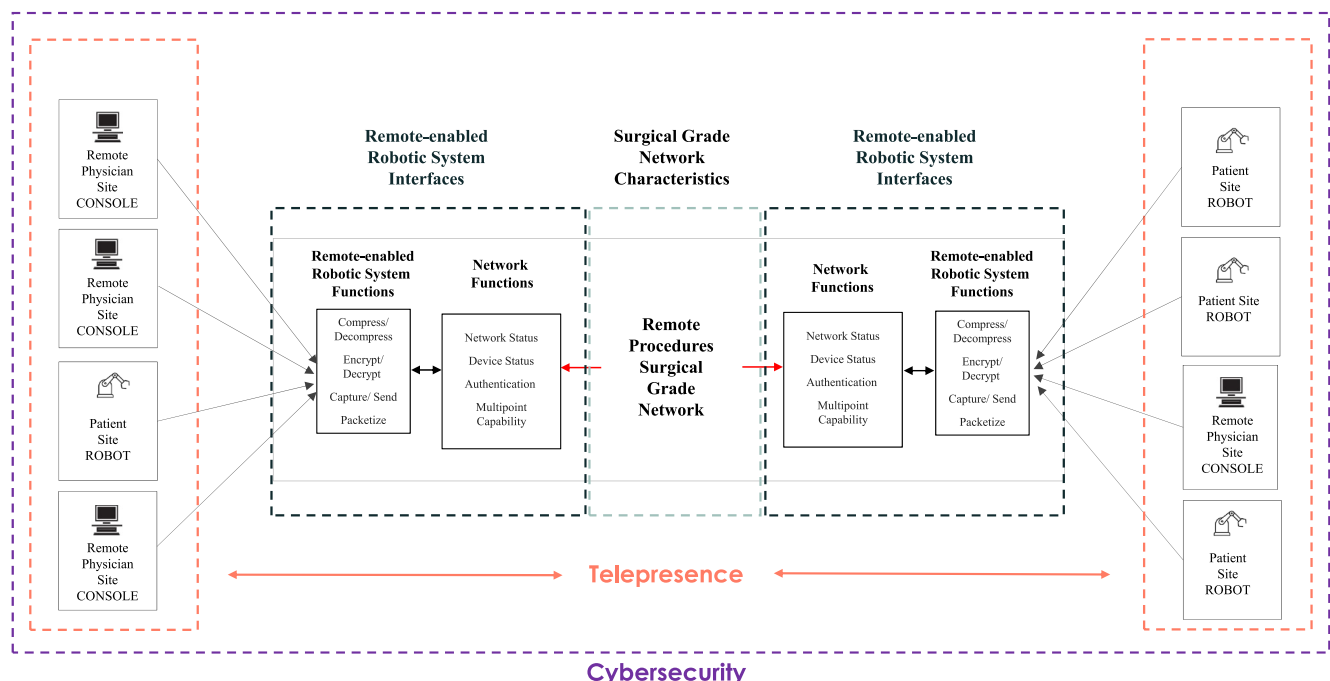


FIGURE 1 | Key components addressed in technical guidelines. [Colour figure can be viewed at [wileyonlinelibrary.com](https://onlinelibrary.wiley.com)]

5. Facility-level requirements for both the REMOTE PHYSICIAN site and the PATIENT SITE.

The technical guidelines apply across various clinical settings (e.g., operating rooms and procedure rooms) and USE CASES with instrument control by the REMOTE PHYSICIAN (e.g., remote minimally invasive surgery, remote tele-mentoring, remote endoscopy, remote endovascular, remote interventions, and other diagnostic procedures).

The guidelines specify various levels of requirements using the following terminology:

- “shall” indicates a requirement
- “should” indicates a recommendation
- “may” indicates a permission

The guidelines do not address:

- Clinical personnel, clinical practice guidelines, or procedure scheduling systems.
- Remote procedures that do not involve tele-manipulation of interventional, surgical, or diagnostic tools.
- Scenarios where the surgical robot operates autonomously without direct input or control by a remote operator.
- Broader digital health features, AI integration, or cloud connectivity beyond the immediate needs of REMOTE ROBOTIC-ASSISTED SURGERY AND PROCEDURES.

3 | Terms, Definitions, and Abbreviations

3.1 | Terms and Definitions

For this document, the following terms and definitions apply:

Authorized Model or Configuration: This refers to the authorized REMOTE-ENABLED ROBOTIC SYSTEM that is permitted to connect over the SURGICAL-GRADE NETWORK. The system is defined and monitored by the robot manufacturer.

Bandwidth: The maximum rate of data transfer achievable over a given medium.

Globally Unique Identifier: An identifier assigned to each device on the SURGICAL-GRADE NETWORK, formatted following special conventions to support uniqueness within an organization and across all organizations, creating identifiers such as a Media Access Control address, globally unique identifiers defined in Request For Comments 9562, or other types of globally unique identifiers.

Host: A computer, device, or other endpoint that is connected to and utilizes a given network.

Internet Protocol: A protocol designed for interconnected packet-switched networks, providing for transmitting data blocks

(datagrams) from source to destination using fixed-length addresses and handling fragmentation/reassembly if necessary.

Interoperability: The ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Jitter: This refers to the inconsistency or variation in the time it takes for data packets to reach their destination.

Latency: The time measurement between when a source transmits data and the destination receives the data.

Multipoint Capability: Refers to a network that has two or more HOSTS and allows communication between any combination of HOSTS.

Network Operations Team: This refers to a team that monitors the SURGICAL-GRADE NETWORK, assesses traffic flow and capacity of all SURGICAL-GRADE NETWORK paths, and may be alerted to issues. This team receives and monitors requests, scheduled or in the moment, to ensure that all REQUESTED SESSIONS have the required BANDWIDTH to complete sessions without constraints.

Network Performance Log: This refers to a record of data collected by the SURGICAL-GRADE NETWORK related to the its operational behavior, intended to provide a detailed picture of the SURGICAL-GRADE NETWORK’s functioning.

Network Latency: The time measurement between when a source transmits data over a network and when the source receives a response or acknowledgment from the destination over the network. This is round-trip time (across the network and back).

Non-Well-Known Ports: A Transmission Control Protocol or User Datagram Protocol port greater than 1023 and less than or equal to 65,535.

Other Related Devices: Devices required for a procedure, such as imaging equipment, monitoring equipment, and other devices, that transmit data over the SURGICAL-GRADE NETWORK during the session.

Patient Site: The location or room of the patient undergoing a remote procedure.

Patient Site Care Team: The care team at the PATIENT SITE supporting the remote procedure (e.g., nurses, operating room technicians, anesthesiologists, clinical engineers, and other physicians).

Peak Load Bandwidth: This is the maximum amount of BANDWIDTH that a SURGICAL-GRADE NETWORK leg is expected to support at any given time, considering the combined BANDWIDTH requirements of all projected active sessions.

Path Maximum Transmission Unit Discovery: A standardized technique in computer networking for determining the maximum transmission unit size on the network path.

Real-Time Network Communications: This refers to network communications (e.g., not control loops) where information is transmitted and received with minimal NETWORK LATENCY.

Remote Physician: The physician in a different location from the patient and care team.

Remote Physician Site: The location where the physician is participating in the remote procedure.

Remote Robotic-Assisted Surgery or Procedure: A clinical procedure, including surgery and interventional procedures, in which a physician uses a REMOTE-ENABLED ROBOTIC SYSTEM and SURGICAL-GRADE NETWORK to perform a procedure on a patient in a different location. Also known as “remote surgery,” “remote procedure,” “telesurgery,” and/or “tele-interventions.”

Remote-Enabled Robotic System: This refers to the entire system used for remote procedures, including the robotic system at the PATIENT SITE, the physician's console at the REMOTE PHYSICIAN SITE, and any hardware or software, required to enable a safe and effective procedure over a SURGICAL-GRADE NETWORK connection.

Requested Session: A single requested instance of a remote procedure that is performed using a SURGICAL-GRADE NETWORK—authorized REMOTE-ENABLED ROBOTIC SYSTEM, with defined BANDWIDTH requirements, and an expected time duration to ensure required BANDWIDTH is available for the SESSION.

Session: This refers to a single instance of a remote procedure performed using a REMOTE-ENABLED ROBOTIC SYSTEM, encompassing the time from when the connection is established to when it is terminated.

Session Log: This refers to a record of data related to a specific remote procedure SESSION intended to capture a comprehensive view of the SESSION, including both SURGICAL-GRADE NETWORK and REMOTE-ENABLED ROBOTIC SYSTEM performance.

Surgical-Grade Network: A managed network with high reliability, robust security, and guaranteed quality of service, which supports the requirements of remote procedures as outlined in these guidelines.

Surgical-Grade Network System Interface: Refers to the interfaces between the REMOTE-ENABLED ROBOTIC SYSTEM and the SURGICAL-GRADE NETWORK to implement connection and communication between the robotic system(s) at PATIENT SITE(s) and physician's console(s) at the remote location(s).

Telepresence: Refers to the use of audio–video technologies to create a virtual presence of the REMOTE PHYSICIAN at the PATIENT SITE.

Teleoperation Latency: The time between when the remote surgeon moves the input device to when that surgeon sees motion of the instrument on their monitor showing the video from the PATIENT SITE robotic system.

Use Case: This refers to any remote procedure with control of the REMOTE-ENABLED ROBOTIC SYSTEM by a REMOTE PHYSICIAN, such as remote minimally invasive surgery, remote endoscopy, remote

endovascular procedures, remote interventions, other remote diagnostic procedures, or tele-mentoring with instrument control.

3.2 | Abbreviations

AAMI	Association for the Advancement of Medical Instrumentation
CoS	Class of Service
DAST	Dynamic Application Security Testing
DDoS	Distributed Denial-of-Service
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
GUID	Globally Unique Identifier
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMDRF	International Medical Device Regulatory Forum
IP	Internet Protocol
ISO	International Organization for Standardization
LAN	Local Area Network
MAC	Media Access Control
MDR	Medical Device Regulation (European Union)
NIST	National Institutes of Standards and Technology
PMTUD	Path Maximum Transmission Unit Discovery
QoS	Quality of Service
RAS	Robotic-Assisted Surgery
RFC	Request For Comments
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WAN	Wide Area Network

4 | Existing Standards Applicable to Remote Procedures

This section addresses existing standards relevant to remote procedures, providing a foundation for ensuring patient safety, cybersecurity, and regulatory compliance. It details key

TABLE 1 | Examples of existing standards that may be applicable to remote procedures.

Category	Standard	Region
Communication and interoperability	IEEE/UL 2933:2024	Global
Cybersecurity and data protection	ISO/IEC 27001:2022+A1:2024	Global
	ISO/IEC 19790:2012	Global
	ISO/IEC 24759:2017	Global
	ISO 80001-1	Global
	IEC 81001-5-1:2021	Global
	IEC 62443-3-2	Global
	IEC 62443-3-1	Global
	IEC 62443-4-1:2018	Global
	IEC 62443-4-2:2019	Global
	UL 2900-1:2023	Global
Medical device safety, quality, and risk management	UL 2900-2-1:2023	Global
	NIST 800-53	US
	AAMI SW96:2023	Global
	ISO 13485:2016	Global
	UL 2800-1:2022	Global
	ISO 14971:2019	Global
	IEC 80001-1:2021	Global
Medical device software lifecycle	IEC 80601-2-77:2019	Global
Medical device usability	IEC 62304:2006+A1:2015	Global
	IEC 62366-1:2015+A1:2020	Global

standards and provides examples across various categories, including communication and INTEROPERABILITY, cybersecurity and data protection, medical device quality and risk management, medical device software lifecycle, and medical device usability [14]. Section 5.2.1 provides additional details related to relevant cybersecurity regulations, guidance, and frameworks.

1. Remote procedures and related operations should adhere to applicable local and global standards to ensure patient safety, cybersecurity, and regulatory compliance as required.
2. Local and global standards that may be applicable to remote procedures include, but are not limited to, the standards listed in Table 1.

5 | Technical Guidelines for Remote Procedures

This section outlines the technical guidelines for the SURGICAL-GRADE NETWORK, cybersecurity, REMOTE-ENABLED ROBOTIC SYSTEM INTERFACES, TELEPRESENCE capabilities, and facility-level requirements for both the REMOTE PHYSICIAN SITE and PATIENT SITE to ensure the safe and effective implementation of remote procedure programs.

5.1 | Surgical-Grade Network Characteristics

This section outlines the network requirements for safe and effective remote procedures, emphasizing the need for a SURGICAL-GRADE NETWORK to ensure reliability and maximize uptime. Key characteristics, such as low NETWORK LATENCY, minimal JITTER, minimal to no packet loss, low error rates, and guaranteed BANDWIDTH, are essential for seamless operation and preventing delays that could compromise patient safety [15–17]. Additionally, these guidelines highlight the importance of secure communication and data protection to maintain confidentiality and integrity throughout remote procedures [18].

5.1.1 | General Surgical-Grade Network

5.1.1.1 | Reliable.

1. A SURGICAL-GRADE NETWORK has the highest level of specifications and shall be optimized for use in remote procedures to ensure reliability, minimize loss of service, and maximize uptime.
2. The SURGICAL-GRADE NETWORK shall deliver the specified uptime required for the USE CASE.
3. To maximize uptime, the SURGICAL-GRADE NETWORK shall implement one or more of the following high availability measures:
 - a. Redundancy with backup systems at various levels (e.g., hardware, connectivity, and power) to prevent single points of failure;
 - b. Failover mechanisms that automatically switch to backup systems or alternative routes without noticeable delays or service interruptions;
 - c. Disparate paths to ensure multiple, independent SURGICAL-GRADE NETWORK routes are available for communication;
 - d. Software defined SURGICAL-GRADE NETWORK packet duplication, sending identical data packets via multiple routes to minimize the risk of packet loss during transmission;
 - e. Other high availability measures.

5.1.1.2 | Multipoint Capability.

1. The SURGICAL-GRADE NETWORK shall allow for MULTIPPOINT CAPABILITY, such that any given REMOTE PHYSICIAN console can connect to one of multiple PATIENT SITE robots as deemed necessary by the facilities.
2. The SURGICAL-GRADE NETWORK shall implement industry-standard authentication and authorization mechanisms for all users, REMOTE-ENABLED ROBOTIC SYSTEMS, and other required connected devices to ensure secure communication and prevent unauthorized access.
3. The SURGICAL-GRADE NETWORK shall ensure isolation of communications across each site or SESSION, such that there is no interaction of data between separate sites or SESSIONS.
4. The SURGICAL-GRADE NETWORK may be able to accommodate OTHER RELATED DEVICES or other network services required for the SESSION.

5.1.1.3 | Bidirectionality. The SURGICAL-GRADE NETWORK should deliver consistent, simultaneous, and comparable BANDWIDTH in both directions between the REMOTE PHYSICIAN SITE and PATIENT SITE to ensure control and feedback of critical data based on the USE CASE SESSION requirements.

5.1.1.4 | Encryption.

1. The SURGICAL-GRADE NETWORK traffic shall be encrypted in transit.
2. Sensitive data shall be encrypted at rest.

5.1.1.5 | Session Performance Guarantees.

1. When supporting multiple simultaneous SESSIONS, the SURGICAL-GRADE NETWORK shall maintain the performance and bandwidth of each SESSION.
2. The SURGICAL-GRADE NETWORK shall be capable of receiving a request to allocate specific BANDWIDTH for a designated block of time and may respond if additional BANDWIDTH is available.
3. The SURGICAL-GRADE NETWORK shall allocate necessary BANDWIDTH for a session if the requested BANDWIDTH is available. If the REQUESTED SESSION is allocated, the total BANDWIDTH required shall be available until the SESSION is ended.
4. The SURGICAL-GRADE NETWORK shall notify the requestor of the status of the BANDWIDTH allocation.

5.1.2 | Quality of Service

5.1.2.1 | Network Latency.

1. The SURGICAL-GRADE NETWORK shall provide an indication of NETWORK LATENCY to the REMOTE-ENABLED ROBOTIC SYSTEM regularly.
2. The SURGICAL-GRADE NETWORK shall contribute no more than the specified amount of NETWORK LATENCY for the USE CASE.
3. The SURGICAL-GRADE NETWORK shall regularly monitor and report NETWORK LATENCY metrics to the REMOTE-ENABLED ROBOTIC SYSTEM.

5.1.2.2 | Jitter.

1. The SURGICAL-GRADE NETWORK shall provide an indication of JITTER to the REMOTE-ENABLED ROBOTIC SYSTEM regularly.
2. The SURGICAL-GRADE NETWORK shall contribute no more than the specified amount of JITTER for the USE CASE.
3. The SURGICAL-GRADE NETWORK shall regularly monitor and report JITTER statistics to the REMOTE-ENABLED ROBOTIC SYSTEM.

5.1.2.3 | Packet Loss.

1. The SURGICAL-GRADE NETWORK shall provide an indication of packet loss to the REMOTE-ENABLED ROBOTIC SYSTEM regularly.
2. The SURGICAL-GRADE NETWORK shall contribute no more than the specified amount of packet loss for the USE CASE.
3. The SURGICAL-GRADE NETWORK shall regularly monitor and report packet loss metrics to the REMOTE-ENABLED ROBOTIC SYSTEM.

5.1.3 | Bandwidth

5.1.3.1 | Sufficient.

1. The SURGICAL-GRADE NETWORK shall guarantee consistent specified BANDWIDTH to carry REMOTE-ENABLED ROBOTIC SYSTEM traffic and other required device traffic for authorized SESSIONS.
2. The SURGICAL-GRADE NETWORK may employ methods, such as QoS/CoS, to maintain consistent BANDWIDTH for any given SESSION.
3. The SURGICAL-GRADE NETWORK shall provide sufficient capacity for all scheduled SESSIONS, even if conditions require network traffic to switch to an alternative path to reach the intended destination.

5.1.3.2 | Scalable.

1. The SURGICAL-GRADE NETWORK shall be capable of receiving and responding to requests from the REMOTE-ENABLED ROBOTIC SYSTEM for additional BANDWIDTH during an active SESSION while simultaneously supporting multiple SESSIONS.
2. The BANDWIDTH capacity of the SURGICAL-GRADE NETWORK shall be capable of accommodating the total PEAK LOAD BANDWIDTH forecast at any given time.
3. The SURGICAL-GRADE NETWORK should have a reserved percentage of capacity above and beyond the PEAK LOAD BANDWIDTH to ensure that unforeseen spikes in utilization and higher than average growth and adoption rates can be accommodated appropriately.

5.1.4 | Protocol

1. The SURGICAL-GRADE NETWORK shall use INTERNET PROTOCOL (IP) as its primary transport protocol and adapt as INTERNET PROTOCOLS evolve.
2. The SURGICAL-GRADE NETWORK shall use Ethernet (IEEE 802.3) for Layer 2 communications to connect the SURGICAL-GRADE NETWORK SYSTEM INTERFACE to the REMOTE-ENABLED ROBOTIC SYSTEM.

5.1.5 | Management

5.1.5.1 | Visibility.

1. The SURGICAL-GRADE NETWORK shall track and collect network operational statistics.
2. The SURGICAL-GRADE NETWORK shall include operational statistics for NETWORK LATENCY, JITTER, packet loss, and BANDWIDTH.
3. The SURGICAL-GRADE NETWORK should collect and track other operational statistics and metrics such as BANDWIDTH utilization (e.g., used for specific SESSIONS and devices), device access and authorization, and other SESSION metrics.

5.1.5.2 | Real-Time Status.

1. The SURGICAL-GRADE NETWORK shall convey appropriate real-time operational status and changes in network conditions

to the REMOTE-ENABLED ROBOTIC SYSTEM, the REMOTE PHYSICIAN site, PATIENT SITE CARE TEAMS, and the NETWORK OPERATIONS TEAM to ensure ongoing safety and security of the remote procedure.

- 2. Recipients of real-time SURGICAL-GRADE NETWORK status updates should interpret the information and respond accordingly.
- 3. The SURGICAL-GRADE NETWORK shall deliver updates at a specified frequency, ensuring that recipients can respond effectively.

5.1.5.3 | Reporting.

- 1. The SURGICAL-GRADE NETWORK shall collect required network operational statistics and provide access to these records on a query basis to the REMOTE-ENABLED ROBOTIC SYSTEM manufacturer, REMOTE PHYSICIAN SITE, PATIENT SITE CARE TEAMS, and NETWORK OPERATIONS TEAM.
- 2. Reported SURGICAL-GRADE NETWORK operational statistics may include NETWORK LATENCY, JITTER, BANDWIDTH utilization, redundancy status, and packet loss.
- 3. Remote SESSION LOGS shall be recorded, retained as required, and accessible to authorized parties.

5.1.5.4 | Operational Control. The SURGICAL-GRADE NETWORK shall effectively manage BANDWIDTH and network traffic while proactively anticipating network utilization to ensure consistency and optimal performance of the SESSION.

5.2 | Cybersecurity

This section addresses cybersecurity requirements for remote procedures, emphasizing compliance with existing regulations, guidance, and frameworks while addressing unique cybersecurity risks (as e.g., through the exposure to third party and/or public networks) introduced by remote procedures [19–23]. Rather than relying solely on traditional cybersecurity best practices, this approach identifies cybersecurity gaps and suggests applicable security practices to be considered when a procedure is performed remotely. Beyond reducing the risk of security compromise, these guidelines also prioritize maintaining patient confidence by mitigating concerns about the safety of remote procedures. Best practices from organizations, such as the FDA and NIST are referenced, ensuring a comprehensive and adaptable approach to cybersecurity in remote procedures. See related Sections 4 for cybersecurity standards and (Appendix A2) for a list of general threats that a REMOTE-ENABLED ROBOTIC SYSTEM should defend against to address and reduce risks associated with the data and systems used in remote procedures.

5.2.1 | Existing Cybersecurity Regulations, Guidance, and Frameworks

- 1. Existing cybersecurity regulations shall be followed as applicable.
- 2. Existing cybersecurity guidance and frameworks should be followed as applicable.

- 3. Cybersecurity regulations, guidance, and frameworks that may be applicable to remote procedures include, but are not limited to, the following examples shown in Table 2.

5.2.2 | Guidelines for Cybersecurity

5.2.2.1 | Introduction of a Third-Party Surgical-Grade Network Provider.

- 1. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer shall design the REMOTE-ENABLED ROBOTIC SYSTEM for defense in depth and assume the SURGICAL-GRADE NETWORK infrastructure between the REMOTE PHYSICIAN console and the PATIENT SITE robot is hostile and may, at any given time, experience compromise or disruption.
- 2. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer shall implement the necessary security controls to ensure the confidentiality, integrity, and availability of data traveling between the REMOTE PHYSICIAN console and the PATIENT SITE robot.
- 3. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer shall integrate failsafe mechanisms and safety controls to protect the patient, users, property, and the environment from harm.
- 4. The SURGICAL-GRADE NETWORK provider shall implement the required security and operational controls to ensure that network performance, uptime, and QoS metrics required

TABLE 2 | Examples of existing cybersecurity regulations, guidance, and frameworks that may be applicable to remote procedures (see Table 1 for cybersecurity standards).

Category	Regulations, guidance, and frameworks
Regional market approval	FDA Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions (2023) FDA Postmarket Management of Cybersecurity in Medical Devices (2016) FDA 21 CFR Part 820 HIPAA 45 CFR Part 160, Part 164 EU GDPR EU MDR
Global development	IMDR/CYBER WG/N70FINAL:2023 NIST SP 800-131A Rev. 2 (2019) IETF TLS 1.3 Protocol ISO/IEEE 11073-40101:2022 ISO/IEEE 11073-40102:2022 FIPS 140-3
Premarket risk	FDA CFR 820.50 AAMI TIR 57:2016
Cybersecurity	AAMI TIR 97:2019 NIST 800-161r1 IETF TLS 1.3 Protocol

for remote procedures are not adversely impacted by either malicious actors or systemic failures. These controls shall address:

- a. Confidentiality protections (e.g., segregation of all REMOTE-ENABLED ROBOTIC SYSTEM SESSIONS);
- b. Integrity protections (e.g., using Message Authentication Codes to verify that the data has not been altered during transmission);
- c. Availability (e.g., protection against and response to DDoS attacks, BANDWIDTH congestion, and infrastructure failures);
- d. Performance and Reliability (e.g., NETWORK LATENCY minimization, JITTER control, and real-time failover);
- e. Disaster Recovery and Business Continuity (e.g., redundancy, geo-distributed backups, and rapid recovery).

5.2.2.2 | Multitenant Nature of the Surgical-Grade Network.

1. The REMOTE-ENABLED ROBOTIC SYSTEM shall employ best practices to mutually authenticate connections and communications between its remote-enabled robotic subsystems to prevent unintended communications.
2. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer and the SURGICAL-GRADE NETWORK shall implement end-to-end encryption between all network nodes.
3. The REMOTE-ENABLED ROBOTIC SYSTEM shall implement end-to-end encryption between all endpoints on the SURGICAL-GRADE NETWORK.
4. The REMOTE-ENABLED ROBOTIC SYSTEM shall employ encrypted protocols from the REMOTE PHYSICIAN SITE console and PATIENT SITE robot to any and all external network services.
5. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer should implement additional data privacy protections to protect personal and sensitive data, considering that hospital-based security controls commonly implemented to keep data private may not be present on the third-party providers' SURGICAL-GRADE NETWORK.
6. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer, and where applicable the SURGICAL-GRADE NETWORK provider, shall ensure that steps are taken to isolate each site/system/user's infrastructure and equipment, including the REMOTE-ENABLED ROBOTIC SYSTEM from untrusted connections by other systems or unauthorized access by other users.

5.2.2.3 | Lack of Physical Proximity Between the Surgeon and Patient.

1. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer, in coordination with the SURGICAL-GRADE NETWORK provider, shall implement security controls that ensure the correct components (e.g., REMOTE PHYSICIAN console and PATIENT SITE remote-enabled robot) are being paired.
2. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer may make use of a shared "SESSION key" that is communicated between the REMOTE PHYSICIAN and the patient-site team and shared "out of band" (e.g., an alpha and/or numeric code that needs to be verbally communicated between the parties). The correct SESSION key shall be required to initiate

communication between the REMOTE PHYSICIAN console and the PATIENT SITE robots.

5.2.2.4 | Potential Introduction of Adverse Effects Through Security Controls.

1. The REMOTE-ENABLED ROBOTIC SYSTEM's security controls shall be evaluated to ensure that they do not lead to an uncontrolled or undesired change in system behavior (e.g., undesirable additional TELEOPERATION LATENCY, JITTER, or worst-case unexpected movement).
2. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer's design shall include measures to reduce the risk of security failures as well as mechanisms for handling errors and exceptions. Any failures shall be addressed through fail-safe features, ensuring that they do not cause undesirable system behavior or disrupt an ongoing procedure.

5.2.2.5 | Robust and Secure Surgical-Grade Network Operations.

The NETWORK OPERATIONS TEAM should evaluate industry best practices for cybersecurity, including but not limited to the following:

1. Implement SURGICAL-GRADE NETWORK security tools to aid with the detection (e.g., NDR, Network Detection and Response or NIDS, Network Intrusion Detection System) as well as Security Incident and Event Monitoring (SIEM) to collectively enable the timely detection, analysis, and response to anomalous traffic and events;
2. Implement SURGICAL-GRADE NETWORK and security log retention capability to meet regulatory and operational requirements;
3. Implement node-level security protections such as Endpoint Detection and Response (EDR) or equivalent protections;
4. Implement a policy and procedure for risks related to supply-chain, subcontractor, and third party partners/vendors;
5. Conduct regular cybersecurity penetration testing, preferably through a well-recognized neutral third party testing provider;
6. Conduct regular vulnerability scanning and monitoring of the network and connected infrastructure;
7. Develop and maintain an asset database and incident response policy and plan;
8. Implement a regular and recurring security review process that addresses logs and events, changes to asset database (s), access provisioning including changes/adds/deletes/stale-records, and least-privilege requirements.

5.3 | Remote-Enabled Robotic System Interfaces

This section addresses the critical interfaces between the REMOTE-ENABLED ROBOTIC SYSTEM and the SURGICAL-GRADE NETWORK, which are essential for safe and effective remote procedures. It outlines the necessary functions required for connectivity and operation, ensuring reliable communication, secure operation, and efficient management of remote robotic procedures. See

related Section (Appendix A1) for a list of other REMOTE-ENABLED ROBOTIC SYSTEM considerations.

5.3.1 | Functions for Remote-Enabled Robotic Systems to Connect and Operate Over a Surgical-Grade Network

5.3.1.1 | Device ID and System Information.

1. Each device connected to the SURGICAL-GRADE NETWORK shall have a GUID that is communicated to the network for connectivity management and security.
2. All GUIDS shall be cryptographically protected and verifiable through strong cryptographic algorithms.

5.3.1.2 | Data Encryption, Decryption. REMOTE-ENABLED ROBOTIC SYSTEM traffic shall be encrypted at the application layer. (Refer to Section 5.2.2.2.)

5.3.1.3 | Data Packetization. Each device connected to the SURGICAL-GRADE NETWORK shall be able to interface with a standard layer 1–3 network and support PMTUD to prevent fragmentation and optimize data transfer.

5.3.1.4 | Ports.

1. Proprietary communication protocols shall use NONWELL-KNOWN PORTS.
2. Standard communication protocols shall use standard ports.

5.3.1.5 | Protocols.

1. Each device application should communicate using either the TCP or UDP protocol.
2. Devices should use standard security communication protocols and avoid protocols that are considered insecure (e.g., use SSH instead of Telnet, HTTPS instead of HTTP, and TLS 1.2/1.3 with strong cipher suites instead of TLS 1.1).
3. Device applications shall use protocols that can be forwarded across a layer-3 IP network.

5.3.1.6 | Routing and IP Addressing. The SURGICAL-GRADE NETWORK interface for each device shall have a unique IP address for each LAN within a specified REMOTE-ENABLED ROBOTIC SYSTEM.

5.3.1.7 | Ability to React to Changes in Surgical-Grade Network Conditions.

1. The REMOTE-ENABLED ROBOTIC SYSTEM shall notify users of appropriate status changes in SURGICAL-GRADE NETWORK conditions.
2. The REMOTE-ENABLED ROBOTIC SYSTEM and users shall interpret and respond appropriately to status changes in SURGICAL-GRADE NETWORK conditions to ensure safety.

5.3.1.8 | Device Surgical-Grade Network Authentication. Connected devices shall authenticate to the SURGICAL-GRADE NETWORK using industry-recognized standard authentication methods.

5.3.1.9 | Session Start-Up Sequence.

1. A SURGICAL-GRADE NETWORK connection to initiate a SESSION shall only be established if the REMOTE-ENABLED ROBOTIC SYSTEM indicates that the SURGICAL-GRADE NETWORK QoS requirements can be met for the USE CASE.
2. The REMOTE PHYSICIAN SITE console and the PATIENT SITE robot may power up independently and asynchronously.

5.3.1.10 | Session End Sequence. The REMOTE-ENABLED ROBOTIC SYSTEM shall notify the SURGICAL-GRADE NETWORK when the SESSION has been completed, and the SURGICAL-GRADE NETWORK shall acknowledge receipt of the notification.

5.3.1.11 | Disconnected Session. If the SURGICAL-GRADE NETWORK stops detecting communication between the REMOTE PHYSICIAN console and the PATIENT SITE robots, the network shall notify the REMOTE-ENABLED ROBOTIC SYSTEM that no robot-system communication is being detected and the REMOTE-ENABLED ROBOTIC SYSTEM should end the SESSION.

5.3.1.12 | Remote-Enabled Robotic System Onboarding.

1. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer shall authorize specific models or configurations of REMOTE-ENABLED ROBOTIC SYSTEMS, including the BANDWIDTH requirements of that configuration, to connect over the SURGICAL-GRADE NETWORK.
2. The healthcare system shall authorize specific REMOTE-ENABLED ROBOTIC SYSTEM devices of an AUTHORIZED MODEL OR CONFIGURATION to connect with each other over the SURGICAL-GRADE NETWORK.
3. The specific authorized models or configurations of REMOTE-ENABLED ROBOTIC SYSTEM devices shall be communicated to the SURGICAL-GRADE NETWORK.

5.3.1.13 | Remote-Enabled Robotic System Offboarding.

1. REMOTE-ENABLED ROBOTIC SYSTEM operators may deauthorize a specific model or configuration of a REMOTE-ENABLED ROBOTIC SYSTEM from operating over the SURGICAL-GRADE NETWORK.
2. All specific REMOTE-ENABLED ROBOTIC SYSTEM devices in a DE-AUTHORIZED MODEL OR CONFIGURATION shall be deauthorized from operating over the SURGICAL-GRADE NETWORK.
3. The healthcare system may deauthorize a specific model or configuration of a REMOTE-ENABLED ROBOTIC SYSTEM from operating over the SURGICAL-GRADE NETWORK.
4. The specific models or configurations of deauthorized REMOTE-ENABLED ROBOTIC SYSTEM devices shall be communicated to the SURGICAL-GRADE NETWORK.

5.3.2 | Required Data Exchange for Remote-Enabled Robotic Systems to Operate Over a Surgical-Grade Network

5.3.2.1 | Surgical-Grade Network Status and Health. The SURGICAL-GRADE NETWORK shall supply the REMOTE-ENABLED ROBOTIC SYSTEM and other components with performance status

and health statistics to ensure confidence in performance and facilitate risk assessment.

5.3.2.2 | Fleet Status. The REMOTE-ENABLED ROBOTIC SYSTEM and other required devices shall report performance status and health statistics to the SURGICAL-GRADE NETWORK to enable readiness for the planned SESSION.

5.3.2.3 | Session Logs. NETWORK PERFORMANCE LOGS for each SESSION shall be recorded, retained as required, and accessible to authorized parties for forensic analysis, troubleshooting, and other purposes.

5.4 | Telepresence

This section addresses the critical role of TELEPRESENCE in remote procedures. It emphasizes the necessity of high-quality REAL-TIME NETWORK COMMUNICATIONS consisting of two-way video and audio between the REMOTE PHYSICIAN SITE and the PATIENT SITE procedure room. These requirements are essential for maintaining situational awareness, ensuring patient safety, and facilitating a seamless workflow when the REMOTE PHYSICIAN and patient are physically separated [24].

5.4.1 | Video in Remote Physician Site and Patient Site Procedure Rooms

1. The REMOTE PHYSICIAN SITE shall have an adequate view of the patient, other participants, and critical monitors and displays at the PATIENT SITE via TELEPRESENCE to ensure safety and facilitate seamless workflow.
2. The room-to-room video connection between the REMOTE PHYSICIAN SITE and the PATIENT SITE procedure room shall be transmitted over a SURGICAL-GRADE NETWORK or a network of equivalent reliability as defined in Section 5.1.1.1.
3. The REMOTE PHYSICIAN SITE should have the capability to access multiple room views as needed for the USE CASE.
4. The REMOTE PHYSICIAN SITE should have the pan, tilt, and zoom capabilities for optimal visualization of the PATIENT SITE monitors and displays as needed per the USE CASE.
5. Participants in the PATIENT SITE procedure room should have an adequate view of the REMOTE PHYSICIAN.
6. The REMOTE PHYSICIAN and care team members may be notified if the room-to-room video connection is lost during a SESSION.

5.4.2 | Audio in Remote Physician Site and Patient Site Procedure Rooms

1. The REMOTE PHYSICIAN SITE shall have the capability of REAL-TIME NETWORK COMMUNICATIONS consisting of two-way audio, with participants in the PATIENT SITE procedure room to maintain situational awareness, ensure safety, and facilitate seamless workflow.

2. The REMOTE PHYSICIAN SITE shall be able to hear critical equipment sounds, including electrocautery signal settings, activation indicators, and fault alerts, within the required timeframe.
3. Audio communications between the REMOTE PHYSICIAN SITE and PATIENT SITE participants shall be transmitted over a SURGICAL-GRADE NETWORK or a network of equivalent reliability as defined in Section 5.1.1.1
4. The REMOTE PHYSICIAN and care team members shall be notified if audio communication is lost during a SESSION.

5.5 | Remote Physician Site and Patient Site Facilities

1. The REMOTE PHYSICIAN SITE and PATIENT SITE shall ensure the REMOTE-ENABLED ROBOTIC SYSTEM is authorized for clinical use in remote procedures by the relevant authority (e.g., the FDA).
2. The REMOTE PHYSICIAN SITE and PATIENT SITE shall comply with all applicable federal, state, and international laws, regulations, guidelines, and standards.
3. The REMOTE PHYSICIAN SITE and PATIENT SITE shall establish comprehensive plans and policies for information privacy and security compliance in remote procedures and ensure that contracts or agreements for remote procedure support include specific security controls for information security management.
4. The REMOTE PHYSICIAN SITE and PATIENT SITE shall have access to appropriately trained and qualified technical support personnel (e.g., clinical engineers) with knowledge and skills in the maintenance and management of REMOTE-ENABLED ROBOTIC SYSTEMS and remote procedures (e.g., network troubleshooting and fail-safe drills).
5. The REMOTE PHYSICIAN SITE and PATIENT SITE shall ensure proper performance validation testing and maintenance of the REMOTE-ENABLED ROBOTIC SYSTEM infrastructure in accordance with relevant policies and procedures of the relevant governing organizations, manufacturer guidelines, and other industry best practices to ensure the REMOTE-ENABLED ROBOTIC SYSTEM remains safe, effective, and compliant with regulatory requirements.
6. The REMOTE PHYSICIAN SITE and PATIENT SITE shall ensure the appropriate SURGICAL-GRADE NETWORK infrastructure required for the remote procedure.
7. The PATIENT SITE for a remote procedure shall meet the same space requirements as local procedures and comply with all relevant standards and regulations to ensure safety, sterility, and functionality of the surgical environment.
8. The REMOTE PHYSICIAN SITE shall be a dedicated space equipped with adequate power, ensuring safety, privacy, and comfort.

Author Contributions

Yulun Wang: conceptualization, writing – original draft, writing – review and editing. **Martin Buehler:** writing – review and editing. **Shane Farritor:** writing – review and editing. **Yuman Fong:** writing –

review and editing. **Mike Kijewski:** writing – review and editing. **Brian Miller:** writing – review and editing. **Bill Peine:** writing – review and editing. **Blair Whitney:** conceptualization, writing – original draft, writing – review and editing. **Mike Yramategui:** writing – review and editing. **Jordana Bernard:** conceptualization, writing – original draft, writing – review and editing, project administration.

Acknowledgments

The authors gratefully acknowledge the following individuals for their invaluable contributions to the development of the technical guidelines: **Contributors:** Russell Berger, Vice President, Product Security and Network Operations, Intuitive Surgical; Seth Carmody, VP Regulatory Strategy, MedCrypt; Phil Dang, Senior Director, Head of Product Security, Information Security and Risk Management, Johnson & Johnson MedTech; Dustin Eastman, Director of Product Security, Technical Fellow R&D, Systems Center of Excellence, Product Security, Medtronic; Dennis Fowler, CMO, Sovato; Brian Gaither, Director, Network Engineering, Sovato; Sheng Lu, Staff Engineer, Virtual Incision; Austin Miller, Cybersecurity Intern, Sovato; Cynthia H. Perazzo, CEO and Co-Founder, Sovato; Marc Tibbitts, Senior Technical Project Manager, Sovato; Walter Martín Villalba, Founder & CEO, C13 Security; Axel Wirth, Chief Security Strategist, MedCrypt; and James Wright, Head of Technical Programs, Sovato. **Content Reviewers (no payment or support provided):** Erik Bond, VP, Enterprise Architecture, Northwell Health; Christophe Chautems, CTO and Cofounder Nanoflex Robotics; Jaesoon Choi, CEO, LN Robotics, Professor of Biomedical Engineering, Asan Medical Center/University of Ulsan College of Medicine; Joseph Cutrell, Director of Strategy and Innovation in the Global Business Division, AT&T; Christopher Difiglia, Director, Enterprise Communications, Northwell Health; Sara Dodd, Staff Design Control Engineer & Group Lead, CMR Surgical; Dieter Flubacher, Software Development, Nanoflex Robotics; Antonello Forgiione, General Director, IRCAD France, Hôpitaux Universitaires de Strasbourg; Brian Korrow, Senior Director, Infrastructure Services and Management, Northwell Health; Robert Nockowitz, Senior Director, Infrastructure Services and Management—CCIE Emeritus #15410, Northwell Health; Riccardo Oliva, IRCAD France; Gynecologic Oncology Unit, Fondazione Policlinico Universitario A. Gemelli IRCCS, Università Cattolica del Sacro Cuore; Paul Pak, AVP, Infrastructure Services and Management, Northwell Health; Thomas Parent, CIO, IRCAD France; Vip Patel, Medical Director, Global Robotics Institute, Advent Health Celebration, Medical Director, Advent Health Cancer Institute Urologic Oncology Program, Professor of Urology, University of Central Florida School of Medicine, Clinical Associate Professor of Urology Nova Southeastern University; Alice Segato, Medical Robotics Engineer, Nanoflex Robotics; Chetan Sharma, Founder and CEO, Chetan Sharma Consulting; Hongjun Sun, Product R&D Director, Shanghai Microport Medbot (Group); and Kuang Zhao, Senior Operations Manager, CSA Group.

Conflicts of Interest

Yulun Wang declares Teladoc Fellow, Cottage Health Board Member, World Telehealth Initiative Chairman and Cofounder, stock options Sovato; Martin Buehler declares stock options Johnson & Johnson; Shane Farritor declares stock and patents Virtual Incision; Yuman Fong declares scientific consultant for Medtronic, Johnson & Johnson, and Imugene, receives royalties from Merck and Imugene, and owns patents for CF33-OVs and CF33-CD19t licensed to Imugene LTD; Mike Kijewski declares none; Brian Miller declares stock options Intuitive Surgical; Bill Peine declares stock, stock options, patents, and grant funding from Office of Naval Research, Grant 14143260, SC 1000020614, “Advanced Tele-Robotic Surgery for Combat Casualty Care;” Blair Whitney declares stock options Sovato; Mike Yramategui declares stock options Intuitive Surgical; and Jordana Bernard declares stock options Sovato.

Data Availability Statement

The authors have nothing to report.

References

1. J. G. Meara, A. J. M. Leather, L. Hagander, et al., “Global Surgery 2030: Evidence and Solutions for Achieving Health, Welfare, and Economic Development,” *Lancet* 386, no. 9993 (2015): 569–624, [https://doi.org/10.1016/s0140-6736\(15\)60160-x](https://doi.org/10.1016/s0140-6736(15)60160-x).
2. T. Uribe-Leitz, M. M. Esquivel, N. Y. Garland, K. L. Staudenmayer, D. A. Spain, and T. G. Weiser, “Surgical Deserts in California: An Analysis of Access to Surgical Care,” *Journal of Surgical Research* 223 (2018): 102–108, <https://doi.org/10.1016/j.jss.2017.10.014>.
3. K. K. Taylor, A. M. Ibrahim, and J. W. Scott, “A Proposed Framework for Measuring Access to Surgical Care in the United States,” *JAMA Surgery* 157, no. 12 (2022): 1075–1077, <https://doi.org/10.1001/jamasurg.2022.3184>.
4. J. Marescaux, J. Leroy, F. Rubino, et al., “Transcontinental Robot-Assisted Remote Telesurgery: Feasibility and Potential Applications,” *Annals of Surgery* 235, no. 4 (2002): 487–492, <https://doi.org/10.1097/0000658-200204000-00005>.
5. M. Anvari, “Remote Telepresence Surgery: The Canadian Experience,” *Surgical Endoscopy* 21, no. 4 (2007): 537–541, <https://doi.org/10.1007/s00464-006-9040-8>.
6. P. Barba, J. Stramiello, E. K. Funk, F. Richter, M. C. Yip, and R. K. Orosco, “Remote Telesurgery in Humans: A Systematic Review,” *Surgical Endoscopy* 36, no. 5 (2022): 2771–2777, <https://doi.org/10.1007/s00464-022-09074-4>.
7. K. E. Georgiou, E. Georgiou, R. M. Satava, “5G Use in Healthcare: The Future Is Present,” *Journal of the Society of Laparoendoscopic Surgeons* 25, no. 4 (2021): e2021.00064, <https://doi.org/10.4293/jsls.2021.00064>.
8. S. K. Reddy, S. Saikali, A. Gamal, et al., “Telesurgery a Systematic Literature Review and Future Directions,” *Annals of Surgery* (2024).
9. D. Itchhaporia, “The Evolution of the Quintuple Aim: Health Equity, Health Outcomes, and the Economy,” *Journal of the American College of Cardiology* 78, no. 22 (2021): 2262–2264, <https://doi.org/10.1016/j.jacc.2021.10.018>.
10. World Health Organization, Global Patient Safety Action Plan 2021–2030: Towards Eliminating Avoidable Harm in Health Care (May 2025), <https://www.who.int/publications/i/item/9789240032705>.
11. V. Patel, S. Saikali, M. C. Moschovas, et al., “Technical and Ethical Considerations in Telesurgery,” *Journal of Robotic Surgery* 18, no. 1 (2024): 40, <https://doi.org/10.1007/s11701-023-01797-3>.
12. M. Mori, S. Hirano, K. Hakamada, et al., “Clinical Practice Guidelines for Telesurgery 2022: Committee for the Promotion of Remote Surgery Implementation, Japan Surgical Society,” *Surgery Today* 54, no. 8 (2024): 817–828, <https://doi.org/10.1007/s00595-024-02863-5>.
13. B. Rocco, M. C. Moschovas, S. Saikali, G. Gaia, V. Patel, and M. C. Sighinolfi, “Insights From Telesurgery Expert Conference on Recent Clinical Experience and Current Status of Remote Surgery,” *Journal of Robotic Surgery* 18, no. 1 (2024): 240, <https://doi.org/10.1007/s11701-024-01984-w>.
14. National Institute of Standards and Technology (NIST 800-53: Cybersecurity Framework (CSF) 2.0, U.S. Department of Commerce, May 2025), <https://doi.org/10.6028/NIST.CSWP.29>.
15. S. Xu, M. Perez, K. Yang, C. Perrenot, J. Felblinger, and J. Hubert, “Determination of the Latency Effects on Surgical Performance and the Acceptable Latency Levels in Telesurgery Using the dV-Trainer(R) Simulator,” *Surgical Endoscopy* 28, no. 9 (2014): 2569–2576, <https://doi.org/10.1007/s00464-014-3504-z>.
16. H. Morohashi, K. Hakamada, T. Kanno, et al., “Construction of Redundant Communications to Enhance Safety Against Communication Interruptions During Robotic Remote Surgery,” *Scientific Reports* 13, no. 1 (2023): 10831, <https://doi.org/10.1038/s41598-023-37730-9>.

17. A. Nankaku, M. Tokunaga, H. Yonezawa, et al., "Maximum Acceptable Communication Delay for the Realization of Telesurgery," *PLoS One* 17, no. 10 (2022): e0274328, <https://doi.org/10.1371/journal.pone.0274328>.
18. K. Kaur, S. Garg, G. Kaddoum, et al., "Secure Authentication and Key Agreement Protocol for Tactile Internet-Based Tele-Surgery Ecosystem ICC 2020 – 2020," *IEEE International Conference on Communications* (2020): 1–6.
19. U.S. Department of Health and Human Services Food and Drug Administration, Postmarket Management of Cybersecurity in Medical Devices Guidance for Industry and Food and Drug Administration Staff (May 2023), <https://www.fda.gov/media/95862/download>.
20. U.S. Department of Health and Human Services Food and Drug Administration, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff (2016), <https://www.fda.gov/media/119933/download>.
21. E. Barker and A. Roginsky, Technology NIOsa 2019 Transitioning the Use of Cryptographic Algorithms and Key Lengths (May 2025), <https://doi.org/10.6028/NIST.SP.800-131Ar2>.
22. J. Boyens, A. Smith, N. Bartol, et al., Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022), <https://doi.org/10.6028/NIST.SP.800-161r1>.
23. T. M. Corporation, Playbook Threat Modeling Medical Devices (2021), <https://www.mitre.org/sites/default/files/2021-11/Playbook-for-Threat-Modeling-Medical-Devices.pdf>.
24. J. W. Collins, A. Ghazi, D. Stoyanov, et al., "Utilising an Accelerated Delphi Process to Develop Guidance and Protocols for Telepresence Applications in Remote Robotic Surgery Training," *European Urology Open Science* 22 (2020): 23–33, <https://doi.org/10.1016/j.euros.2020.09.005>.
25. Bonaci T., Herron J., Yusuf T., et al., "To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robots," *arXiv:1504.04339* (May 2015).
26. S. Iqbal, S. Farooq, K. Shahzad, A. W. Malik, M. M. Hamayun, and O. Hasan, "SecureSurgiNET: A Framework for Ensuring Security in Tele-surgery," *International Journal of Distributed Sensor Networks* 15, no. 9 (2019): 1550147719873811, <https://doi.org/10.1177/1550147719873811>.

Appendix A

A1 | Other Remote-Enabled Robotic System Considerations

This section outlines additional technical design and implementation considerations for REMOTE-ENABLED ROBOTIC SYSTEMS to ensure the safety and effectiveness of remote procedures beyond the core guidelines discussed in previous sections. These considerations highlight important factors for adapting existing robotic systems to function remotely and address specific challenges introduced by network-dependent operations.

1. Ensuring TELEOPERATION LATENCY, which will vary by REMOTE-ENABLED ROBOTIC SYSTEM and distance between the remote physician site and PATIENT SITE, is acceptable for a given use case.
2. Ensuring the REMOTE-ENABLED ROBOTIC SYSTEM can tolerate (per the SLA of the SURGICAL-GRADE NETWORK) SURGICAL-GRADE NETWORK properties, such as NETWORK LATENCY, JITTER, and packet loss. Ensuring the REMOTE-ENABLED ROBOTIC SYSTEM can reestablish a connection after a SESSION timeout. Designing system acknowledgments, such as heartbeats and command statuses, to prevent timeouts given the TELEOPERATION LATENCY. Testing the system at maximum TELEOPERATION LATENCY to confirm the system's ability to handle potential timeouts effectively.
3. Ensuring that the REMOTE-ENABLED ROBOTIC SYSTEM can adjust parameters based on dynamic SURGICAL-GRADE NETWORK conditions.

Adaptability to changing SURGICAL-GRADE NETWORK conditions while maintaining performance. The REMOTE-ENABLED ROBOTIC SYSTEM notifying the REMOTE PHYSICIAN of degrading SURGICAL-GRADE NETWORK conditions that may affect performance.

4. Ensuring the start-up sequence of the REMOTE-ENABLED ROBOTIC SYSTEM accounts for the separation between the remote console and the rest of the system. Designing the remote console and the PATIENT SITE robot to boot up independently, ensuring seamless operation despite their physical separation. Integrating this independent startup process into the system's design to accommodate SURGICAL-GRADE NETWORK constraints and maintain functionality.
5. Utilizing a low-loss low-LATENCY codec for endoscopic video or imaging, as it serves as the primary feedback mechanism for remote procedures. This approach preserves high-quality visuals, ensuring that video quality is indistinguishable from that of same-room imaging.
6. Ensuring energy source control remains reliable and tolerant of communication degradation and failures. Implementing a fail-safe design and clear indications of the device status and settings to enable effective awareness for the remote user.
7. Ensuring PATIENT SITE clinicians have the capability of halting the REMOTE SITE physician's control of the remote-enabled robot when necessary, serving as a critical safety mechanism.
8. Allowing both the REMOTE PHYSICIAN SITE and PATIENT SITE to pause or temporarily interrupt instrument control during the procedure when necessary, enhancing overall safety.
9. Ensuring a safe, seamless, and definitive transition of control between a remote console and another console.
10. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer ensures controls and visible warnings are implemented to prevent physical injury when the PATIENT SITE staff enter the movement safety zone of articulating components during a remote procedure.
11. The REMOTE-ENABLED ROBOTIC SYSTEM manufacturer implements a method for the PATIENT SITE staff to quickly pause remote movement control, bidirectional audio–video; and terminate a remote SESSION without automatic remote reconnection.

A2 | General Threats a Remote-Enabled Robotic System Should Defend Against

In addition to the cybersecurity gaps covered in Section 5.2, developers of REMOTE-ENABLED ROBOTIC SYSTEMS should adhere to established best practices for identifying, enumerating, and defining requirements for cybersecurity risks. Specifically, threat modeling must be performed to analyze and mitigate risks associated with both the overall REMOTE-ENABLED ROBOTIC SYSTEM architecture and its individual components [25, 26]. Additionally, the following key security practices address and reduce risks to the confidentiality, integrity, and availability of the data and systems, regardless of their remote capabilities:

1. Compliance with generally accepted security requirements and security engineering best practices.
2. Implementation of plans and processes for cybersecurity premarket and postmarket risk management, including identification, communication, and mitigation of new risks as well as securing and distributing software updates and patches.
3. Follow generally recognized security principles (e.g., Secure by Design, Secure by Default, Least Privilege, and Defense in Depth).
4. Follow best practices for software security review and analysis, including threat modeling, attack surface analysis, software composition analysis, code review, and SBOM vulnerability analysis.
5. Follow best practices for software testing, including robustness testing, static application security testing (SAST), dynamic

application security testing (DAST), boundary value analysis, fuzz testing, vulnerability scanning, and penetration testing.

6. Provide evidence of testing at the respective integration stages and for the total system, including traceability of security requirements and identified risks to test results.
7. Formalize and document any decisions regarding risks resulting from identified vulnerabilities that could not be or were not mitigated.
8. Formalize and document any security trade-off decisions (e.g., security vs. safety, security vs. usability, and security vs. features).
9. Provide documentary evidence supporting the above security practices.
10. User instructions and diagrams pertaining to cybersecurity, such as secure installation and integration, SURGICAL-GRADE NETWORK requirements, security infrastructure requirements, and security incident response handling.
Remote procedures, by definition, introduce a data path that sends command and control data for REMOTE-ENABLED ROBOTIC SYSTEMS outside the hospital network. This data path introduces the potential for heightened risks. Some related threats to consider include:
 11. Attacks on external SURGICAL-GRADE NETWORK infrastructure, impeding the availability and real-time capabilities of these systems.
 12. A man-in-the-middle attack on an external data center.
 13. Compromise of personal or sensitive data as it leaves the hospital's network.

Networks used for remote procedures should be designed with threats, such as these in mind, and built with mitigation strategies to anticipate these risks.

(See Section 5.2 for cybersecurity guidelines and requirements for remote procedures).