Surgical Endoscopy (2019) 33:684–690
https://doi.org/10.1007/s00464-018-06631-8

SAGES/EAES OFFICIAL PUBLICATION

# White paper: technology for surgical telementoring—SAGES Project 6 Technology Working Group

**Etai M. Bogen**[1] · **Christopher M. Schlachta**[2] · **Todd Ponsky**[3,4]

Received: 14 November 2018 / Accepted: 17 December 2018 / Published online: 7 January 2019


## Abstract

**Background** Recent advances in telecommunication technology and video conferencing systems have opened a new avenue for surgical instruction called "surgical telementoring." This report from the Technology Working Group of the SAGES Project 6 Summit reviews the telementoring technology that currently exists and proposes recommendations for minimum technology requirements and future technology development. While also providing insight in regulatory considerations, this review offers what prospective surgical telementoring participants need to know about the underlying technology with a specific focus on safety, reliability, transmission quality, ease of use, and cost.

**Methods** Content experts from around the world, in minimally invasive surgery, surgical mentoring and telementoring, surgical education, business development, healthcare innovation, and regulation were invited to attend a 2-day summit in Los Angeles, USA to outline the current state of surgical telementoring and chart the challenges and opportunities going forward. This article summarizes the discussion, conclusions, and recommendation of the technology group with regard to telementoring technology.

**Results** This article reviews the technical requirements which can be divided into the following categories: (1) safety, (2) reliability, (3) transmission quality, (4) ease of use, and (5) cost.

**Conclusion** Telementoring applications are technology driven. Given the pace of change of technology, guiding principles in technology design and selection are warranted (Table 4). Telementoring technologies require two basic components, video capturing and display devices at the transmitting and receiving end, and a telecommunication link between them. Many additional features can be added to this basic setup including multiple cameras or video sources, remote camera zoom and pan, recording and storage of videos and images, and telestration capabilities to mention just a few. In general, the cost of these technologies is feature driven. The education framework for each specific application should determine the need for these features (Schlachta in Surg Endosc https://doi.org/10.1007/s00464-016-4988-5).

**Keywords** Telementoring · Mentoring · Technology · Minimally invasive surgery · Laparoscopy

Recent advances in telecommunication technology and video conferencing systems have opened a new avenue for surgical instruction called "surgical telementoring" (ST). In 2015, The Society of American Gastrointestinal and Endoscopic Surgeons (SAGES) defined Telementoring as "a relationship, facilitated by telecommunication technology, in which an expert provides guidance to a less experienced learner from a remote location" [1]. As this concept of virtual surgical teaching has become a reality, SAGES convened the Project 6 Summit in Los Angeles, California. At Project 6, five focus groups were established to review the state of the art and develop guiding principles for moving forward with this promising platform. The Technology working group (Table 1) reviewed the telementoring technology that currently exists and defined recommendations for technology requirements and future development.

✉ Etai M. Bogen
etaibogen@me.com

1 Department of Clinical Medicine, Faculty of Health Sciences - University of Tromsø, Tromsø, Norway

2 Department of Surgery, Schulich School of Medicine and Dentistry, Western University, London, Canada

3 Division of Pediatric Surgery, Akron Children's Hospital Akron, One Perkins Square, Akron, OH 44308, USA

4 Department of Pediatric Surgery, Cincinnati Children's Hospital, Cincinnati, USA

**Table 1** Project 6 Summit technology opportunities participants

| | |
|---|---|
| Etai Bogen, MD Co-Lead | University Hospital of Northern Norway |
| Ozanan Meireles, MD Co-Lead | Massachusetts General Hospital USA |
| Ted Trus, MD Co-Lead | Dartmouth–Hitchcock Medical Center |
| Marc Schwachter, MD | GlobalCastMD |
| Paul Szotek, MD | IU Health |
| Helena Mentis, MD | Health IT and Human-Centered Computing |
| Moji Ghodoussi, PhD | Intouch Health |
| Leslie Landrum | Karl Storz |

## Methods

Content experts from around the world, in minimally invasive surgery, surgical mentoring and telementoring, surgical education, business development, healthcare innovation, and regulation were invited to attend a 2-day summit in Los Angeles, USA to outline the current state of surgical telementoring and chart the challenges and opportunities going forward. This article summarizes the discussion, conclusions, and recommendation of the technology group with regard to telementoring technology.

IRB approval is not needed for this paper.

## Results

Description for the desired telementoring device.

Technical requirements can be divided into the following categories: (1) safety, (2) reliability, (3) transmission quality, (4) ease of use, and (5) cost.

### Safety and data security

Any device that is taken into the operating room and used in a clinical setting requires several levels of approval to ensure patient and staff safety and uphold strict data security. The two main regulatory vehicles in charge of this in the US are the Food and Drug Administration (FDA) and Health Insurance Portability and Accountability Act (HIPAA).

#### FDA classification for medical devices

The FDA's mission includes protecting the public health by assuring the safety, efficacy, and security of medical devices [2]. This mission is expansive, and the FDA takes a correspondingly expansive approach in its regulation of medical devices in order to achieve it. The FDA regulates medical devices based on the risk and innovation associated with the device. Under this scheme, the FDA designates devices as Class I (lowest risk), Class II (moderate risk), or Class III (highest risk). These classes correspond with the level of regulation that applies to the device. Generally, Class I devices can enter the market without any pre-approval or clearance by FDA, while Class II devices must comply with premarket notification requirements including a 510(k) submission. This is in addition to other regulatory requirements such as quality system requirements and medical device reporting among others. Finally, Class III devices must submit and obtain approval for a premarket approval application ("PMA") before they can be sold in the marketplace. In general, a PMA takes longer duration, is more expensive, and requires more clinical data than a 510(k) submission [3].

FDA has classified many patient monitoring devices as Class II devices, including general hospital and personal use monitoring devices, anesthesiology monitoring devices, obstetrical and gynecological monitoring devices, and cardiovascular monitoring devices. Telemedicine devices with similar patient monitoring uses (e.g., telestroke, tele-ICU, among others) also are typically regulated as Class II devices. Current telementoring technology devices are developed only by handful manufacturers and are classified as a Class II device [3]. Certification for a Class II medical device is a tedious process which is both time consuming and incurs high costs.

**Regulation of mobile health technologies** The FDA regulations for telemedicine devices and software are very similar to the HIPAA requirements but more specific for telemedicine [3].

Medical device data systems (MDDS): In February 2011, FDA issued a regulation for MDDS devices, it is defined as "A device that is intended to provide one or more of the following uses, without controlling or altering the functions or parameters of any connected medical devices: (i) the electronic transfer of medical device data; (ii) the electronic storage of medical device data; (iii) the electronic conversion of medical device data from one format to another format in accordance with a preset specification; or (iv) the electronic display of medical device data." MDDS are devices through which medical device data are passively transferred or communicated. They do not modify, interpret, or add value to the data or the display of the data. Importantly,

MDDS devices may include software or electrical hardware but do not include devices intended to be used in connection with active patient monitoring. A device that involves active patient monitoring is any device that

- is intended to be relied upon in deciding to take immediate clinical action;
- involves detection, measurement, or recording of patient data and other functions of a patient monitoring device; and
- transmits, stores, converts, or displays medical device data that are intended to be relied upon in deciding to take immediate clinical action or that are to be used for continuous monitoring by a healthcare professional, user, or the patient.

For example, a telemedicine device used in conjunction with scheduled, routine patient care where immediate clinical action is not required could be regulated as a Class I MDDS device. To the extent that such a device uses two-way audio/video technology merely to capture and transmit patient-specific data, the device would maintain its Class I designation. However, where the manufacturer intends for the device to be used in active patient monitoring, a higher classification would be required. The FDA applies the MDDS regulation to anyone who manufactures an MDDS device, including healthcare facilities—e.g., a hospital, physician practice, or clinical—acting as manufacturers [3].

Mobile Medical Applications: After finalizing the MDDS regulation, the Agency expanded its efforts to other aspects of mobile health and telemedicine. In July 2011, the FDA published a draft guidance on the regulation of mobile medical applications, in which the Agency described its current thinking on the regulation of software designed for a mobile platform and intended for use in the diagnosis, treatment, or prevention of disease [3].

Types of regulated mobile apps include the following:

- Apps that "connect to" one or more medical device(s) for purposes of controlling the device(s) or displaying, storing, analyzing, or transmitting patient-specific medical device data.
- Apps that transform the mobile platform into a medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices.
- Apps that use algorithms that output a patient-specific result, diagnosis, or treatment recommendation to be used in clinical practice.

Clinical decision support software: The FDA also has begun to explore regulation of clinical decision support (CDS) software. Though not yet officially defined, the Agency has described CDS as "Any software, whether designed as a mobile application, web-based service or desk top application, that uses an individual's information from various sources (electronically or manually entered) and that converts this information into new information that is intended to support a clinical decision" [3].

The FDA has given examples of CDS to include look-up databases, comparison algorithms, and simple calculators (e.g., software that produce an index or score based on known formulae). This expansive meaning suggests that FDA believes it can regulate any software that interprets *any* "actionable information" from virtually *any* source if the information or the result of the interpretation is intended to be used in the clinician's decision-making process [3].

**Health Insurance Portability and Accountability Act (HIPAA) requirement and regulations** Guidelines on telemedicine are very clear on how sensitive patient information should be transferred and handled during a remote session from any distance. The HIPAA regulations cover three main areas: physical, administrative, and technical. In order to be HIPAA-compliant, it is required that communication of protected health information at distance must be fully compliant in each of these categories [4].

The *physical* HIPAA guidelines on telemedicine concern the security of the computer systems at both ends of the line on which encrypted health information is maintained and the environment in which the computer systems are located. Responsibilities included in the physical requirements involve establishing an alternative/redundancy plan in the event of a crisis or emergency situation and implementing validation procedures to limit physical access to the computer systems [3].

The *administrative* HIPAA requirements call for system administrators to be appointed in each medical facility to develop formal best practices for the selection and implementation of a secure messaging solution. Administrators are responsible for introducing appropriate policies to guide the conduct of healthcare professions using the secure messaging solution and for monitoring usage of the solution to identify any potential breach of sensitive patient data [3].

This *technical* requirement covers the processes and controls that have to be put in place in order to protect sensitive patient data while in transit. These include the following:

1. Each healthcare professional that is authorized to use the secure messaging platform must be issued with a unique username and password in order to authenticate their identity when accessing or communicating protected health information at distance.
2. The secure messaging platform must be configured in such a way that communications can only be transmitted within a defined private network (VPN) and that sensi-

tive patient data contained within the communications cannot be copied, pasted, or forwarded.
3. The secure messaging platform must be able to monitor activity by authorized users and have the facility to remotely delete and/or retract any transmitted communication that may result in the compromise of sensitive patient data.

**Data security and data encryption recommendations** There is a diversity of local security requirements of the different institutes across the world. Several solutions can be combined to meet the high security demands of both of the regulatory bodies and local institutes:

1. Simple ways to increase data security should be considered at first. For example, enabling WPA2 encryption on a wireless device enhances the security of information transmitted over wireless networks, but it must be enabled on the mobile device, tablets, and mobile PCs [5].

   Alternatively or in addition to securing the wireless network a VPN (Virtual Private Network) or end-to-end secure tunnel is a highly secure way to assure that only authorized individuals connect and access the video/audio transmission. This also reduces the possibility for unauthorized access to the network and for disruption the transmission. VPNs are currently used frequently by Internet and eHealth communities [6].
2. Encryption of data is a key component of security that allows for the protection and preservation of anonymity, but it must precede the transfer of data. According to Federal HIPAA and HITECH Act regulations, this key must contain 128 bits for sufficiency security (Department of Health and Human Services 2013) [5].
3. Authentication protocols ensure that the connection is made with the correct participants, that only authorized individuals have access to data and tools, that only valid and protected devices are used, and that data are sent through authorized channels. The use of two-factor authentication, such as with a pin/password and a token/smart card/dongle is one recommended solution [5].

## Reliability and stability

The reliability of all telementoring systems regardless of the type or manufacturer depends on the availability and quality of the network connection. This can be divided into two main categories: (a) bandwidth and (b) latency.

Since telementoring systems facilitate transmission of high-quality video and audio, the bandwidth requirements are high. In networks, bandwidth is defined as the bit rate of available or consumed information. This capacity is typically expressed in metric multiples of bits per second. As shown in Table 2, the minimum bandwidth for telementoring should be around 40 megabits per second (Mbits/s) as found in a T3 line. Telementoring can be achieved with lower bandwidth but high-quality audio and video might lag and be choppy.

Another aspect of reliability of telementoring systems is latency. Latency is defined as the time interval a package of data travels between two points and back or, from a more general point of view, a time delay between the cause and the

**Table 2** Bandwidth for common communication technology

| Bandwidth | Example of facilitating devices | Suitability for telementoring |
|---|---|---|
| 56 kbit/s | Modem/dialup | Not suitable for telementoring |
| 1.5 Mbit/s | ADSL | |
| 1.544 Mbit/s | T1/DS1 | |
| 10 Mbit/s | Ethernet | |
| 11 Mbit/s | Wireless 802.11b | |
| 24 Mbit/s | ADSL2+ | |
| 44.736 Mbit/s | T3/DS3 | Recommended bandwidth for telementoring |
| 54 Mbit/s | Wireless 802.11 g | |
| 100 Mbit/s | Fast ethernet (most common) | |
| 600 Mbit/s | Wireless 802.11n | |
| 1 Gbit/s | Gigabit ethernet | |
| 1.3 Gbit/s | Wireless 802.11ac | |
| 2.5 Gbit/s | Optical carrier 48 | Recommended for institutes with multiple telementoring systems and simultaneous transmissions / for support in HD/4K future systems |
| 5 Gbit/s | USB 3.0 | |
| 10 Gbit/s | 10 Gigabit ethernet, USB 3.1 | |
| 100 Gbit/s | 100 Gigabit ethernet | |

kbit/s: kilobits per second, Mbit/s: megabits per second, Gbit/s: gigabits per second

effect of some physical change in the system being observed. From a technology point of view, the latency can be divided into the following three main categories:

### Latency generated by the device

This latency is a constant. It is generated by the hardware itself and cannot be controlled, modified, or influenced. Latency generated by hardware is typically very low (< 50 ms) and is not counted in the overall latency calculations. The hardware latency expected from low end devices is usually quite high and results in a lag in the local display of the images in the operating room.

### Latency generated by the network

The network latency depends on many factors such as network type, number of users using the network in a specific time, the number of devices connected, and the type and volume of data packages sent in a given moment.

### Latency generated by software

Telementoring similar to video conferencing depends on a codec to *co*mpress and *dec*ompress the video. This will be discussed in further detail later.

Low latency is crucial in telementoring live cases so that mentors can be temporally aware and potentially able to counsel against evolving intraoperative complications. Based on the experience of the Technology Working Group, it is recommended that total latency does not exceed 450 ms.

### SAGES recommendation

For live telementoring with annotation, we recommend a total latency < 450 ms.

## Transmission quality

### Resolution

One of the first concepts to understand when comparing standard definition (SD) and high definition (HD) is resolution (Table 3). "Resolution is defined as the maximum number of distinct pixels that can be displayed in an image"[7]. Pixels are the smallest point or dot that display color in an image.

### Frame rate

In motion pictures, television, and in computer video displays, the frame rate is the number of frames or images that are displayed per second. Several factors affect the actual frame rate one observes on a computer. For example, a personal computer processor or graphics hardware may only be capable of playing 10–15 frames per second without hardware acceleration.

### Codec

A codec is a device or software for encoding and/or decoding a digital data stream or signal. A codec compresses the data so that it requires less bandwidth. There is a trade-off between codec speed and bandwidth which is balanced by adjusting the video resolution and frame rate.

In North America, SD resolution is 640 × 480 pixels and HD resolution is either 1280 × 720 or 1920 × 1080 pixels. Video quality can be affected by how the image is scanned and displayed. Interlaced video divides horizontal lines across images into odd and even that refresh alternately, whereas progressive video displays lines in sequence from top to bottom to create a sharper picture. Consequently, the letter "i" or "p" is often added to dimensions to define resolution further (e.g., 1280 × 720 p) [8]. The most widely used coding structures today is H.264/AVC encoder, namely x264 [9].

**Table 3** Illustration of frame rate, bandwidth compression ratio

| | Transport bandwidth required | Resolution | Frame rate | |
|---|---|---|---|---|
| | Uncompressed | Compressed | | |
| Standard definition (SD) | 9 Mbps | 128 kbps | QCIF (176 × 144) | 15 fps |
| | 36 Mbps | 384 kbps | SCIF (256 × 192) | 30 fps |
| | 71 Mbps | 512 kbps | 4CIF (512 × 384) | 15 fps+ |
| | 144 Mbps | 768 kbps | 4CIF (512 × 384) | 30 fps |
| High definition (HD) | 332 Mbps | 1 Mbps | HD720 (1280 × 720) | 15 fps+ |
| | 664 Mbps | 2 Mbps | HD720 (1280 × 720) | 30 fps |
| | 1.4 Gbps | 3 Mbps | HD720 (1280 × 720) | 60 fps |
| | 1.5 Gbps | 4–6 Mbps | HD1080 (1920 × 1080) | 30 fps |

**Table 4** Summary of recommendations for telementoring technology

| |
|---|
| Telementoring systems and solution should comply with FDA Class II device and HIPAA regulation |
| Wireless networks should be enabled with WPA2 encryption and in addition a VPN (Virtual Provider Network) or end-to-end secure tunnel is a highly secure way for the appropriate authorized personal to high-sensitive data |
| A minimum 128-bit encryption and Authentication protocols to ensure that the connection made is associated with the correct participants |
| The minimum bandwidth for telementoring should be around 40Mbit/s |
| Video transmission and distribution should be of low latency without packet losses that might lead to choppiness and pixilation. Accepted total latency should be < 450 ms |
| Standard definition (SD) resolution is suited and sufficient for telementoring, a minimum, a resolution of 480 lines of progressive scan resolution (480 p) at 15 frames per second (standard definition) but ideally a resolution of 1080 progressive scan (1080 p) at 30 frames per second |
| Telestration and annotation are desired features and essential for surgical education |
| Telementoring system should be portable and affordable |

Increasing either resolution or frame rate increases the network traffic burden. Although video compression algorithms do a good job of reducing bandwidth consumption, they create latency since compressing and decompressing the data takes time. Some solutions use specific hardware that handle this task and reduce the latency. Finding a good telementoring system means finding a system that can balance bandwidth with resolution, frame rate, and compression/decompression.

#### Recommendation

The ideal image quality depends on the specific telementoring application. A resolution of 480 lines of progressive scan resolution (480 p) at 15 frames per second (SD) is the minimal requirement but may not allow appreciation of fine detail. Ideally, a resolution of 1080 progressive scan (1080 p) at 30 frames per second should accommodate the most sophisticated telementoring application.

### Ease of use

#### Interactive capability

Telementoring without the ability to point on the screen is inadequate. Telestration (tele-illustration) and video annotation are technologies that allow the mentor to virtually draw on the mentees video screen to enhance communication.

**SAGES recommendation** Any surgical telementoring technology should have telestration capability [10].

#### Portability

Integrated suites with built in telementoring capabilities are a luxury item and should be considered in new OR design. Telementoring systems that are easily portable from one operating room to another will allow smaller, budget conscious centers to utilize one unit in service of several operating rooms.

#### Video recording

Although not necessary for telementoring, reviewing, debriefing and coaching with recorded surgery has an important role in the learning process. Video recording capabilities should be built into any telementoring system.

### Cost

Telementoring system prices are variable. Prices can be as low as $3000 USD to as high as $100,000 USD. The return on investment of telementoring is currently not well defined. It is an ongoing challenge to justify large investments in telementoring systems. Sophisticated and expensive systems are widely available. Low-cost systems that will be HIPAA compatible and FDA compliant are most needed for small institutes or developing nations where telementoring for advanced surgical techniques are also needed.

## Conclusion

Telementoring applications are technology driven. Given the pace of change of technology, guiding principles in technology design and selection are warranted (Table 4).

Telementoring technologies require two basic components, video capturing and display devices at the transmitting and receiving end, and a telecommunication link between them. Many additional features can be added to this basic setup including multiple cameras or video sources, remote camera zoom and pan, recording and storage of videos and images, and telestration capabilities to mention just a few. In general, the cost of these technologies is feature driven. The education framework for each specific application should determine the need for these features [1].

## Compliance with ethical standards

**Disclosures** Dr. Ponsky reports personal fees from Conmed, other from GlobalCastMD, outside the submitted work. Dr. Bogen, Dr. Schlachta have no conflicts of interest or financial ties to disclose.

## References


1. Schlachta CM, Nguyen NT, Ponsky T, Dunkin B (2016) Project 6 Summit: SAGES telementoring initiative. Surg Endosc. https://doi.org/10.1007/s00464-016-4988-5
2. FDA's mission statement. Retrieved from (2004) https://www.fda.gov/downloads/aboutfda/reportsmanualsforms/reports/budgetreports/ucm298331.pdf
3. FDA: Medical device classifications and regulation. http://www.fda.gov/MedicalDevices. Accessed 6 Jul 2016
4. HIPAA Administrative Simplification Statute and Rules. http://www.hhs.gov
5. NIAAA (2015) Privacy and security in mobile health (mHealth) research. Alcohol Res: Curr Rev 36:1–10
6. Adibi S, Wickramasinghe N, Chan C (2013) The cloud computing paradigm for mobile health. Int J Soft Comput Softw 3:403–410
7. Robin M (2005) Horizontal resolution: pixel or lines, vol 1. Broadcast Engineering
8. Liu W-L, Zhang K, Locatis C, Ackerman M (2011) Internet-based videoconferencing coder/decoders and tools for telemedicine. Telemed e-Health 17:358–362. https://doi.org/10.1089/tmj.2010.0193
9. Panayides A, Eleftheriou I, Pantziaris M (2013) Open-source telemedicine platform for wireless medical video communication. Int J Telemed Appl 2013:1–12. https://doi.org/10.1155/2013/457491
10. Bogen EM (2014) Telementoring in education of laparoscopic surgeons: an emerging technology. WJGE 6:148–149. https://doi.org/10.4253/wjge.v6.i5.148