

Guideline

Open Access



White paper: requirements for routine data recording in the operating room

Thomas Schnelldorfer^{1,2} , Andrew A. Gumbs³ , Jennifer Tolkoff⁴, Sarah Choksi⁵, Jessica Stockheim⁶, Amin Madani⁷, Carla M. Pugh⁸ , Takeaki Ishizawa⁹ , Stefanie Speidel¹⁰ , Lee L. Swanström¹¹ , Bettina M Rau¹², Amir Szold¹³ , Fabio Ausania¹⁴ , Filippo Filicori^{5,15}, Roland Croner⁶, S. Vincent Grasso¹⁶

¹Surgical Imaging Lab, Tufts Medical Center, Boston, MA 02111, USA.

²Data Intensive Studies Center, Tufts University, Medford, MA 02155, USA.

³Département de Chirurgie Digestive, Centre Hospitalier Intercommunal de Poissy/Saint-Germain-en-Laye, Poissy 78300, France.

⁴Office of General Counsel, Tufts Medicine, Burlington, MA 01803, USA.

⁵Intraoperative Performance Analytics Laboratory, Department of General Surgery, Lenox Hill Hospital, Northwell Health, New York, NY 10075, USA.

⁶Department of Surgery, University of Magdeburg, Magdeburg 39106, Germany.

⁷Department of Surgery, University of Toronto, Toronto M5G 2C4, Ontario, Canada.

⁸Department of Surgery, Stanford University, Stanford, CA 94305, USA.

⁹Department of Hepatobiliary-Pancreatic Surgery, Graduate School of Medicine, Osaka Metropolitan University, Osaka 545-8585, Japan.

¹⁰Division of Translational Surgical Oncology, National Center for Tumor Diseases Dresden, Dresden 01307, Germany.

¹¹Institute for Image-Guided Surgery, IHU Strasbourg, Strasbourg 67000, France.

¹²Klinikum Neumarkt, Neumarkt 92318, Germany.

¹³Assia Medical Group, Assuta Medical Center, Tel Aviv 69710, Israel.

¹⁴Department of HPB and Transplant Surgery, Hospital Clinic, IDIBAPS, Universitat de Barcelona, Barcelona 08036, Spain.

¹⁵Donald and Barbara Zucker School of Medicine at Hofstra/Northwell Health, Hempstead, NY 11549, USA.

¹⁶Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131, USA.

Correspondence to: Dr. Thomas Schnelldorfer, Surgical Imaging Lab, Tufts Medical Center, 800 Washington St, Boston, MA 02111, USA. E-mail: thomas.schnelldorfer@tufts.edu

How to cite this article: Schnelldorfer T, Gumbs AA, Tolkoff J, Choksi S, Stockheim J, Madani A, Pugh CM, Ishizawa T, Speidel S, Swanström LL, Rau BM, Szold A, Ausania F, Filicori F, Croner R, Grasso SV. White paper: requirements for routine data recording in the operating room. *Art Int Surg* 2024;4:7-22. <https://dx.doi.org/10.20517/ais.2023.34>

Received: 25 Sep 2023 **First Decision:** 19 Dec 2023 **Revised:** 22 Dec 2023 **Accepted:** 12 Jan 2024 **Published:** 22 Jan 2024

Academic Editor: Hengrui Liang **Copy Editor:** Pei-Yun Wang **Production Editor:** Pei-Yun Wang

Abstract

This white paper documents the consensus opinion of the authors and *Artificial Intelligence Surgery* editorial board members regarding common requirements needed to implement routine recording of data in the operating room. The statements were agreed upon by all authors and they attempted to outline common barriers that need to be



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose, even commercially, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.



addressed when implementing such recordings.

Keywords: Data recording, domain-specific interconnectivity, cloud-based storage, deidentification, coding of data, data access, automated features

INTRODUCTION

To properly train, test, and validate any system that utilizes artificial intelligence (AI) in surgery, the existence of large, high-quality datasets is critical^[1,2]. Some of the data can come from the preclinical setting, but much of the data is expected to derive from routine clinical care settings, such as the operating room. Therefore, now more than ever, there is a keen interest in the routine recording of data in the operating room. This comes with a broad range of potential benefits, such as retrospective reviews of intra-operative findings to guide post-operative care, the development of new adjunct technologies, such as AI systems, increased transparency in the identification of areas of need, and intelligent tools for training and providing feedback^[3]. However, these potential benefits also come with tremendous ethical concerns and barriers, which in the past have been the main roadblock to more widespread adoption and implementation of AI in healthcare. The goal of this manuscript is to identify the common requirements needed to address these barriers and to implement methods for the reliable recording of useful data in the operating room and thereby create a realistic pathway for wider implementation.

When it comes to recording data in the operating room, it is important to separate data that is created as part of the standard of care from the data that is not a product of this routine care [Table 1]. The latter falls under the well-established regulations of research and will not be addressed in this manuscript. This manuscript will mainly focus on the data created as part of the standard of care of patients, but that is not routinely recorded. Routinely recorded data created as part of the standard of care, such as the anesthesia record, can frequently outline a workable pathway and could be considered as a case example that can be replicated for data that is not routinely collected. A review of the literature reveals that most authors have focused on the routine recording of endoscopic videos. However, the same processes apply equally to the other data commonly produced in the operating room.

It is important to mention that this manuscript is not intended to be a global “recipe” for how to implement routine recording in the operating room. The goal of this manuscript is to identify the common requirements that need to be addressed (i.e., the “what”), but does not provide concrete solutions (i.e., the “how”). It is crucial to recognize that the rules of legitimate implementation of routine recording can differ amongst various jurisdictions or even cultural settings. The actual solutions for implementation can further vary depending on the data type to be recorded, the purpose for recording, the institutional environment, geographical culture, and local standards of care.

METHODS

Members of the Editorial Board of *Artificial Intelligence Surgery* were tasked with identifying the principal requirements for routine data recording in the operating room and drafting a White Paper of guidelines. This OR Data Recording Task Force consisted of T.S, AAG, and SVG. The issues were divided into nine main categories: (1) Consent Process; (2) Technical Requirements; (3) Data Use and Access (Clinical, Research and Innovation, Education, Quality Improvement, and Access); (4) Data Privacy and Security (Privacy and Confidentiality, and Cybersecurity); (5) Data Retention; (6) Data Ownership; (7) Governance; (8) Financial Cost; and (9) Impact on Medical Malpractice Claims. Experts in the field of OR data recording were identified by the Task Force members and were also asked to write some of the sections. Statements

Table 1. Examples of types of data available in the operating room (examples can vary by practice)

| | Data created as part of standard of care | Data NOT routinely created as part of standard of care |
|------------------------------------|--|--|
| Data routinely recorded | <ul style="list-style-type: none"> • Vital signs • Most radiographic images • Selected device data (e.g., ventilation) • Administrative (e.g., supplies) | <ul style="list-style-type: none"> • Research |
| Data NOT routinely recorded | <ul style="list-style-type: none"> • Patient data (e.g., images, video, audio) • Device data (e.g., table position, energy device electric resistance measures, stapler pressure measurements, etc.) • Surgeon data (e.g., kinematics, eye tracking) • Healthcare team interactions (e.g., operating room “black box”) | <ul style="list-style-type: none"> • Research |

were extracted from each section by the Task Force. All the authors (OR Data Registration Task Force and Invited Experts) of the White Paper approved the statements prior to submission of the manuscript for publication.

Consent process

Patient consent is an important aspect of routine recording in the operating room and, by default, should be obtained prior to recording. The format of the consent process can vary depending on jurisdiction and institutional policies, but also on the purpose of recording. While under certain circumstances, a waiver of written consent might be allowed, for most situations, incorporation of the consent for recording is going to be part of the consent for the planned operation or part of the consent for a specific research study. Rare exceptions of informed consent might apply, such as patients who are not competent to provide consent in the absence of a proxy or guardian, life-threatening emergencies with inadequate time to obtain consent, or patients who voluntarily waive their right to consent^[4]. Care must be taken when obtaining consent from vulnerable populations, such as patients undergoing emergency or urgent operations, intellectually disabled people, children, the elderly, pregnant women, socioeconomic and/or educationally disadvantaged people, and prisoners.

Regarding the consent format, it should be “informed” and follow typical standards such as subjective standards, reasonable patient standards, or reasonable physician standards, which are usually determined by the local jurisdiction^[4]. It should include explanations of the type of data to be recorded, what the data will and will not capture, the handling and storage of the data, the scope of use of the data, access to data and sharing of data, the associated risk and benefit, and alternative options. It needs to address potential conflicts, such as healthcare pressure on the patient who wants an operation and fears to not upset the care team or any benefit the consenting clinician may obtain from recording, *etc.* It should include whether the data will be shared with the patient routinely, by request, or not at all. This consent should be a palatable presentation to a patient facing a major life event. Therefore, careful consideration should be given to the level of detail included in the consent. Additionally, it may also take into account the unforeseeable unknowns regarding potential AI applications in the future.

In particular, the decision of whether or not the data will be shared with the patient is a complex issue. If data is shared, either routinely or by request, setting the patients’ expectations for what they will likely encounter when they see the data is beneficial. For example, if the data is a video of the operation, it would be important to explain to the patient before the operation that the video may show bleeding, minor errors, other imperfections, and the involvement of the entire team, including trainees. Typically, there is a great disconnect between patient expectations and surgical reality. After the operation, a process of explaining the data to the patient before it is shared is needed. For example, for an operative video, it can be helpful for a qualified member of the surgical team to go over the video with the patient and be available for any

questions that arise thereafter. In general, patients may need to be prepared for the potentially emotional response they may experience when they encounter such information. Sharing of recorded data with patients, therefore, can come with a substantial time commitment for the surgical team.

Additional considerations include whether members of the surgical team need to be consented if their participation in the operation is captured by the recording^[5]. Issues concerning implicit consent by the surgeon and care team as part of their employment need to be reviewed. Opt-out options not only for the patient but also for the surgeon and care team should be implemented. Handling of any data, if consent were to be withdrawn after recording takes place, needs to be predetermined. Furthermore, in case the data is not de-identified, a more stringent/detailed consent might be needed. Additionally, the associated increase in workload needs to be addressed depending on who is consenting and leading discussions and whether there is any potential need for additional written information.

Statement - Consent process

1. Patient informed consent is an important aspect of routine recording in the operating room and, by default, should be obtained prior to the initiation of recording.
2. Patient informed consent should include whether or not the data will be shared with the patient routinely, by request, or not at all.
3. If the data is a video of the operation and if data is shared, it would be important to prepare the patient for what is expected to be seen.
4. Whether or not members of the surgical team need to provide consent prior to being recorded, given that their participation in the operation is also captured, needs to be decided and clearly defined prior to any recording in the OR.

Technical requirements

The requirements for any recording device to be used in the operating room ultimately depend on the type of data to be recorded, the proposed goals, and regulatory requirements. However, it almost always includes the capability to collect raw digital data from various output sources. Surgical teams, therefore, need to be familiar with the distinct types of digital data. Capturing data within the operating room includes both juxta-operative and circum-operative data sources. The juxta-operative domain includes the focus of surgical activity represented by the operative procedure itself. The circum-operative domain is represented by all activity outside the direct focus of surgical activity, namely, the physical space occupied by the surgical staff that would afford visual, audio, and environmental data capture. This data is divided into what is physically being recorded and its metadata. Metadata refers to a dataset that provides information related to the actual data set and is typically stored within the actual data set. For example, the metadata of a surgical video may include information such as the patient's name, surgeon's name, date of service, and the type of surgical procedure performed.

The interfaces and connectivity required for the recording of generated data such as video and audio are frequently standardized and divided between analog and digital signals. Interfaces typically utilize connectors that are ubiquitous among consumer electronic devices (e.g., digital: HDMI, DisplayPort, FireWire, Thunderbolt, USB-C; analog RCA jacks, 3.5 mm TRS minijacks).

The recording of video and related data from within the operating room has traditionally been provided by relevant vendors of video cameras and surgical kits. Such vendors have developed platforms enabling features such as auto-deidentification of protected health information, auto-bookmarking, voice control for annotation, wireless connectivity, and preconfigured user profiles with standardized setups. Regardless of

the vendor's configuration, features of the recording device would need to include a wide range of relevant connectors. It requires the ability to control the recording, playback, and annotation of milestones within the operative procedure by way of voice input or via a control on an instrument. The identification or deidentification of the recorded video should be configurable within the file naming convention established. Ideally, recording devices should have the ability to customize file names. File naming conventions should allow for the opportunity for a high-level recognition of the file content. Relevant data could be included within a database schema where a unique identifier would be linked to other relevant data from sources of record such as the electronic medical record. Foregoing the above and deciding not to use vendor-related recording hardware permits the opportunity to configure a more bespoke recording environment, but would require technical resources that may or may not be available to even the software developers.

At the present time, data recording within a digital format is ubiquitous, cost-effective, and does not require advanced technical skill sets. However, the curation of recorded data is a complex business process that requires organizational commitment and resources. Business requirements include, but are not limited to, the assurance that patients' protected health information related to the recorded data is stored appropriately according to privacy and security requirements for the entire lifetime of the data. AI-based deidentification of any protected health information within the data is a helpful tool, but it needs to be vetted for each situation and evaluated for the ability to re-identify. In addition, information including the surgical team involved during the procedure needs to be managed appropriately. Multiple data streams also need to be coordinated or "time-stamped" in order to establish temporal connections. The metadata associated with the recorded data needs to be either programmatically or manually configured based on an agreed standard format. The issue of how to manage the de-identification of recorded data versus the creation of metadata related to the recording needs to be addressed and appropriately managed. This would include discussions concerning the legal ramifications surrounding how the data is labeled, utilized, manipulated, and edited. Assurances of maintaining the original data file in an uncorrupted state would need to be configured and managed for purposes including, but not limited to, medical legal issues. Standards of data structure should be followed.

The recorded data requires a storage system compliant with whichever regulatory framework applies to patient privacy and security [e.g., Health Insurance Portability and Accountability Act (HIPAA) in the United States or General Data Protection Regulation (GDPR) in the European Union]. Utilization of external vendors may require additional legal agreements to ensure compliance with this regulatory framework. On-premise storage or cloud-based storage represent potential sites for digital data storage and access. Typically, a large-capacity storage system is required. Economic and security-related issues are involved in this decision, but the trend over the past 10 years has been the migration of data and systems of record from on premises to the cloud with validated firewall protection. Blockchain technology provides a promising platform for such secure cloud-based storage^[6]. Given the expected large size of routinely recorded data, identifying how much storage space is needed to store uncompressed raw data and, potentially, subsequently processed data under the type of storage structure required is advised and frequently requires a business and research rationale. Access to all relevant data requires control mechanisms that are usually established. Hence, the transfer of data between end users and storage sites would follow standard secure access protocols currently implemented and mandated by relevant regulatory authorities. This could include two-factor authentication over a virtual private network or VPN. Special consideration is required when the recorded data will be tied directly to electronic medical records of patients or to other sources of records that contain patient information. In the vast majority of situations, after the data undergoes annotation, it is advisable to store the data either in a de-identified or coded manner. Therefore, a careful decision needs to be made whether the data will be de-identified (no known

link between the data and any protected health information exists) or coded (data does not include any protected health information, yet a separate key to link the data and protected health information exists). Throughout these data transfers, technical and semantic interoperability needs to be maintained to allow for future data exchange.

Human workforce challenges do exist whenever a new workflow process or business responsibility is introduced into business workflows. This involves organization controls via management, workforce training, professional autonomy consistent with the working dynamics between clinicians and management, methods to ensure safeguards, and other related matters. Discussions concerning personal, professional, and organizational risks need to be addressed and managed by appropriate input sources such as the medical legal team members. Training instruction sets need to be developed, tested, refined, and released to ensure staff members are not only fully trained on the recording device but recognize the value generated for all relevant stakeholders, especially patients.

Any device used for routine recording must have the ability to stop automated recording if consent or other criteria are not met.

Statement - Technical requirements

5. The type of recording device used, its connectivity, and its interaction with other devices and workflows need to be carefully assessed on a case-by-case basis.
6. AI-based deidentification of any protected health information within the data is a helpful tool, but it needs to be vetted for each application and evaluated for the potential for re-identification by third parties.
7. Maintaining the data in its original format and uncorrupted state prior to analyses is recommended.
8. The recorded data requires a storage system compliant with whichever regulatory framework applies to patient privacy and security (e.g., HIPAA in the United States or GDPR in the European Union). Utilization of external vendors in this setting may require additional legal agreements to ensure compliance.
9. A careful decision needs to be made whether the data will be de-identified (no known link between the data and any protected health information exists) or coded (data does not include any protected health information, yet a separate key to link the data and protected health information exists).
10. Any device used for routine recording must have the ability to stop automated recording if consent or other criteria are not met.

Data use and access

While the use of routinely recorded data can be numerous, most use cases can fall within the following four themes: (1) clinical; (2) research and innovation; (3) education; and (4) quality improvement. Identifying the proposed use of the data is crucial since it dictates the regulatory processes and also guides processes to minimize systemic biases in the design of data recording.

Clinical

Clinical use cases are typically done for documentation purposes, to allow for retrospective consultation with other healthcare providers, to guide future management (e.g., future decisions that are guided by retrospective review of the data), and for education purposes.

Research and innovation

Most intra-operatively recorded data can also be used for various research and innovation purposes. Such data can help identify unmet needs by assessing the root cause or mechanism of a complication. Similarly, data recordings can be used to assess whether particular interventions (e.g., new device, new technique,

educational course) result in differences in operative-specific metrics (e.g., surgeon performance, operative events, operative time). It is also imperative to recognize that surgical data can be a fairly rich source of raw data. In the case of operative videos, for example, as the field of surgical data science has begun to bloom, AI for computer vision (CV) has led to a new generation of algorithms that are capable of performing high-level tasks such as anatomical identification, tool tracking, and scene recognition^[7,8]. The reality is that the opportunities for innovation from recorded data seem endless.

Education

Another common use of surgical data is for education and quality-improvement purposes. In the case of operative videos, this ranges from coaching, pre-operative rehearsal, post-operative debriefing, quality-improvement conference presentations, self-assessment, credentialing, or creating educational content. Specifically, the use of surgical videos has gained significant popularity over the last two decades as a medium for surgical education, with suggestions that videos might be able to assess performance and provide formative feedback for quality improvement^[9]. While video-based assessment has gained significant momentum as a more objective and relevant method to determine competency and readiness for practice and for obtaining feedback for deliberate practice during surgical training, this has yet to become validated or become mainstream. However, depending on the geographic jurisdictions and surgical subspecialty, credentialing bodies can mandate that for members record their videos for assessment and credentialing purposes. For example, in Japan, it is a requirement for minimally-invasive surgeons to submit their videos through the Japanese Society of Endoscopic Surgeons' Endoscopic Surgical Skill Qualification System^[10]. It is very likely that video-based assessment - whether done for formative feedback or high-stakes summative purposes - will become a common element of most surgical practices in the near future; this highlights the need for routine data recording.

Quality improvement

In addition to the quality benefits gained through research and education, the quality of care can be improved through a responsive review of recorded data after an adverse event occurs. Depending on the jurisdiction, if recordings are maintained for quality improvement and are not disclosed to the patient, there may be avenues available to establish confidentiality and privilege over these recordings (e.g., Patient Safety Organizations). Data access should typically be restricted when used for quality improvement initiatives if data is maintained within a peer review framework.

Access

Decisions about the use case of the recorded data lead to questions about access to the data by various stakeholders. Data access should be determined on a need-to-know basis, which clearly depends on the purpose of the data to be used. A common question that needs to be addressed is whether patients will have access to the data from their own operation or not, and how any access restrictions are being disclosed to patients during the consent or how the data is being shared with the patient in a way that allows the patient to understand the data (e.g., surgeon going over the video recording with the patient). The potential sharing with third parties by a data transfer agreement requires careful review and needs the involvement of a legal or compliance expert, given the typically high degree of legal restrictions, especially if any potential commercial interest is involved. This requires an assessment of whether involved devices from external vendors (e.g., recording devices, storage platforms, etc.) provide the vendor with access to the data, which frequently mandates specific business agreements with the vendor to assure compliance. Third-party sharing is sometimes mandated for regulatory oversight (e.g., institutional/ethical review boards, government officials, etc.) and sometimes desired (e.g., data donation to research institutions). Care must be taken that secure means are available to share the data with third parties if needed. Care must also be taken

if access by third parties (e.g., other academic centers or industry) would impact future intellectual property or licensing claims.

Given the importance of these determinations, an institutional data use and access policy is typically recommended.

Statement - Data use and access

11. Data access should be determined on a need-to-know basis, which clearly depends on the purpose of the data use.
12. The potential sharing with third parties requires careful review and the involvement of a legal or compliance expert, given the multitude of potential legal restrictions and implications.
13. An assessment of whether involved devices from external vendors provide the vendor with access to the data is crucial.
14. Care must be taken that secure means are available to share the data with third parties if needed.

Data privacy and security

Privacy and confidentiality

Routine data recording in the operating room comes with potential challenges in protecting the privacy of any person present. While the patient is likely the most vulnerable party involved requiring protection, care must also be taken to not forget about the privacy of hospital employees. There may be different requirements/considerations depending on the use of the data. Research, for example, may have a different framework than clinical care.

Regarding protection of patient privacy, established laws, such as the GDPR in the European Union, the HIPAA in the United States, and the Electronic Documents Act in Canada, set regulations for personal data collected applicable to the healthcare setting to ensure that data is used in a legitimate manner, kept securely, and only stored for a pre-defined time period^[5]. These regulations, which can vary according to jurisdiction, typically mandate that all subjects involved have to be informed about what happens to their personal data^[5]. Minimizing the recording of any protected health information by choosing the type of data recorded is important. Consent is an important part of the privacy protection process. While many institutions have generalized consent forms that allow for the recording of surgical procedures, some fail to inform the patient about risks involving privacy. Some authors suggest that consent forms should inform the subjects of the purpose of the recording, the risks to their privacy, and how long the data will be stored^[11].

Regarding privacy protection of the operating room team, additional factors need to be considered. These include compliance with workplace privacy rules and assessment of whether routine recording in the workplace can be considered a condition of employment, posing potential issues. Similar to the situation for patient privacy, de-identification or coding of any identifiers involving the operating room team and in particular the surgeon needs to be considered, particularly if an unjust judgment by outside review of the recorded data, like work performance assessment, is a concern. With routine recording, proximate data can inadvertently be captured. For example, in the case of video recording, this can include audio and video, not only of the surgical procedure but of the entire operating room environment. Data capture processes need to address this risk.

Automated deidentification or coding of the data through AI algorithms as part of privacy by design should be considered of high importance^[5]. The risk of re-identifiability of prior de-identified or coded data needs

to be assessed for every system. Common areas where this needs to be addressed are images of faces or other visual identifying features (e.g., tattoos, scars, *etc.*), voices, names, dates, or any other protected health information. These issues become even more important if data is shared with third parties and if the data becomes part of an AI system introduced into clinical care. Technologies known as privacy-enhancing technologies can further help ensure privacy by design while obtaining large amounts of data without compromising privacy^[12]. Such processes should be outlined in an institutional data management policy.

Cybersecurity

Data storage and access lead to areas where data security could be compromised. Data should only be stored and kept for as long as needed for research purposes with limited access by users as outlined by law in most jurisdictions (e.g., HIPAA, GDPR). Data should be stored securely with encryption, password protection, and on a secure server that meets industry standards or in a physically locked area. Identifiers and protected health information should only be stored if relevant to the purpose of the data use, with any identifiers to be deleted as soon as possible. If de-identification is not possible or practical, coding of the data with a separate password-protected master key to separate any identifiers from the rest of the data should be considered so that re-identification by trained personnel can occur for the designed purpose of data use. Again, privacy-enhancing technologies can help ensure data is de-identified before storage. The inclusion of the data into the patients' medical records needs to be decided on a case-by-case basis, but for many applications, such as research, quality improvement, and education, it might not be appropriate^[13].

Access to data recordings should be kept as limited as possible. A secure link for data access to allow editing, annotation, or sharing needs to be assured. Many recent advances in collaborative efforts between scientists and clinicians can take place only if data and annotations are exchanged amongst research teams. Federated learning is a novel way to implement machine learning (ML) while protecting the data privacy of users^[14]. Federated learning permits the training of models while keeping data local, allowing for privacy-preserving data analysis^[15]. While it comes with its own challenges, it can help ensure that researchers are abiding by privacy regulations. Also, connected devices seemingly unrelated to the source or site of storage of data but part of the healthcare Internet of Things can represent a security risk.

Given the vast challenges to cybersecurity with the management of large data provided by routine recording in the operating room, the creation of a data management policy to address these challenges prior to implementation and to ensure all collaborators are able to properly and securely manage the data is crucial. Surgeons and researchers need to be aware of the risks of storage and use of any data with regard to privacy and cybersecurity as technologies continue to change over the coming decade. Insurance coverage for any damages might be considered. Overall, a maintenance plan to address future security threats is important.

Statement - Data privacy and security

15. Minimizing the recording of any protected health information by carefully choosing the type of data recorded is paramount.
16. The risk of re-identifiability of prior de-identified or coded data needs to be assessed for every system.
17. Data should only be stored and kept for as long as needed for research purposes with limited access by users as outlined by law in most jurisdictions.
18. A secure link for data access to allow editing, annotation, or sharing needs to be assured.
19. A maintenance plan to address future security threats is important.

Data retention

Any routine data recording system needs to be compliant with existing institutional data retention policies and local laws. This starts with a solid data maintenance/management plan that outlines how data is stored in a secure manner with periodic updates and reviews. The duration of required or allowed retention of the data can vary depending on the jurisdiction, the purpose of data recording, and whether data is securely de-identified or not. Familiarity with these regulations is mandated. Besides determining when data is deleted, it is also important to establish a mechanism for how the data is physically and digitally discarded without any means of retrieval. This also involves the decision regarding the deletion of data that has been shared with other parties. Further, a plan needs to be established for the rare case of a legal claim requesting access to data that would be considered discoverable, since deletion of discoverable data after a claim has been filed could be considered destruction of evidence. Overall, a data retention policy is recommended to solidify a standardized process.

Statement - Data retention

20. Besides determining when data is deleted, it is also important to establish a mechanism for how the data is physically and digitally discarded without any means of retrieval.

Data ownership

When it comes to the important question of who owns the recorded data, for most jurisdictions, this question is not legally well-defined. While the obvious stakeholders are the surgeon, patient, research team, research institution, and hospital, others dependent on the situation might need to be evaluated, such as the rest of the surgical team, insurance payer, device manufacturer, and analytics manufacturer. The claim is frequently linked to the purpose of recording (research vs. clinical care vs. education). Such evaluations, which are frequently case-specific, also need to consider the consequences of ownership, such as liability, financial responsibility, and regulatory duty. The question about ownership particularly becomes important if the data is used for research that results in a commercial healthcare product where intellectual property protection or licensing becomes a consideration. This is particularly relevant once we recall how Henrietta Lack's pancreatic cancer cell lines (HeLa) were used for decades without the family even being aware or receiving any compensation. Additional consideration is required for ownership of any preprocessed data. Raw patient data is not usually used for AI purposes. Instead, edited, anonymized, and annotated data is what feeds AI algorithms and is probably the most valuable asset in the field. It, therefore, must be determined which stakeholder controls this aspect of the data. Proactive contractual agreements amongst relevant stakeholders can be a method to address any legal ambiguity.

Statement - Data ownership

21. The designation of ownership of the data is ideally defined and determined before any recordings take place, particularly if the data is used for research that might result in a commercial healthcare product where intellectual property protection or licensing becomes a consideration.

22. Proactive contractual agreements amongst relevant stakeholders should be utilized to avoid any future legal ambiguity.

Governance

An important and complex undertaking, such as routine recording in the operating room, mandates detailed oversight from outside the involved team with careful vetting of regulatory requirements. The oversight typically starts prior to implementation, with the supervising entity heavily involved in the design of the undertaking. Even after implementation, proactive surveillance of regulatory compliance by the supervising entity (e.g., monitoring by a hospital's compliance office) is typically mandated.

Various stakeholders need to be considered regarding their role in reviewing and approving the undertaking prior to implementation. However, even after the initiation of routine recording, these reviews typically continue throughout the life of the undertaking with periodic reviews of its activities, policies, and data. Common stakeholders for such oversight include hospital compliance offices, ethics review boards, and various government officials. Under rare circumstances, it may also involve malpractice insurance companies, employee unions, and payers. Such oversight can sometimes go beyond the typical compliance review. Given the potential use of the recorded data for the review of sentinel events, a formal process is required for how the data will be utilized for such reviews if the initial purpose of recording is not directly aimed at quality improvement. While routine review of all data for surgical/clinical errors is typically not mandated and frequently impractical, such practices may become more mainstream in the future. Processes of how to disclose error discovery through the recorded data require definition. In addition, dependent on the use of the recorded data and local legislature, data might become part of medical records and ultimately require the same regulatory oversight.

The burden to ensure competency with new medical devices typically lies with the institution and the user^[13]. Training and sometimes even credentialing of users of routine recording devices, therefore, requires institutional oversight.

Statement - Governance

23. Routine recording in the operating room mandates detailed oversight from outside the involved team with careful vetting of regulatory requirements.

24. Processes of how to disclose error discovery through the recorded data require definition.

25. Training and sometimes even credentialing of users of routine recording devices requires institutional oversight.

Financial cost

When considering systems needed for routine data recording in the operating room, additional costs will occur and need to be addressed in advance. The source of costs can vary depending on individual circumstances. There are typically fixed costs for the installment of data recording systems. This includes the cost of installing hardware and its software, with the total sum depending on the number of recording equipment needed and the quality and number of features of the system. Annual maintenance costs for these systems can be significant. Fixed cost can also include storage systems with their total sum dependent on storage size and type. Fixed cost could also include additional office space for dedicated personnel. There are operating costs related to additional work for non-clinical personnel to conduct data collection, curation, annotation, storage, and data privacy management/governance and for clinical personnel to obtain consent and participate in data collection. Given the typically present infrastructure of an operating room, indirect costs, such as added electricity and required governance, are usually minimal.

While the cost of installing small-scale recording equipment may be covered by a research grant aimed at developing AI-based assessment, comprehensive recording systems usually have to be paid for by the hospital as a facility cost. Times of extension or new development of operating rooms typically present opportunities. Less common funding from malpractice providers of the data is primarily used for quality improvement. Alternatively, if the data is primarily used for education, educational institutions may contribute funding, presenting interesting opportunities. Routine recording, however, can also provide a source of revenue, for example, if the data is used to develop a commercial AI system that could lead to licensing of the data. With the expected cost, the need for funds, and the potential for revenue, it is advisable to develop a business plan.

Statement - Financial cost

26. With the expected cost, the need for funds, and the potential for revenue, the development of a business plan is recommended.

Impact on medical malpractice claims

The availability of additional data from the operating room is expected to directly improve operative patient care, particularly when used for quality improvement processes. However, routine data recording, particularly in a high-stakes environment such as the operating room, raises imminent concerns for misappropriation in the setting of potential medical malpractice claims. The degree of this concern amongst healthcare providers and administrators can vary depending on local legal environments represented by the frequency of malpractice claims in the specific profession and jurisdiction^[16-20]. Further, the impact of certain operative data, such as video recording, on particular court cases is mostly unknown, because of few objective surgical standards, subjective interpretation of operative steps, and paucity of precedence of use in legal cases. It also likely varies amongst jurisdictions depending on factors such as the use of professional judges versus lay juries, jury demographics, and tort reform structure. Even when using such data in the setting of quality improvement, peer review protection is frequently unclear, dependent on local laws and precedents.

In areas where guidelines cannot capture every situation, good surgical care requires individualized and patient-centered approaches, particularly when it comes to emergency cases, end-stage or palliative cases, or complex cases with high-risk profiles or unusual anatomy. Hence, it is difficult and, in some cases, impossible to objectively and reliably interpret data originating from the operating room when used by either the plaintiff or the defendant for a potential malpractice claim. This uncertainty leaves a lot of room for subjective interpretation, which creates the potential for misrepresentation of the operative data in the setting of a claim. It is also not clear if analyzing data that historically has not been routinely recorded even has the capability to answer typical legal questions. AI-based algorithms might have such capability in the future, but clearly not at the current state and do require a blame-free environment to be developed. Such tension is not only a barrier to broad implementation of routine recording, but also could have unforeseen impacts on typical care when routine recording is introduced (e.g., eliminating involvement of trainees, a lower threshold to conduct defensive medicine). The impact on training, in particular, is concerning, since trainees require a supportive teaching environment to go through a learning curve to create surgical confidence where minor errors corrected under qualified surgical supervision are part of the process. Legal exploitation of such minor errors is of particular concern.

Sufficient de-identification of recorded data and conversion of data, without retention of identifiable data or the ability to re-identify, may place data outside of available discovery and may provide a solution to the concerns around claims. However, it may also limit the use of the data for other purposes. In this context, the decision to store the data separately from the patient medical records needs to be evaluated along with the strength of any applied de-identification process (i.e., the risk for re-identification through AI in a large data set is theoretically possible). On the other hand, keeping data discoverable could facilitate its use for the surgeon to better communicate with the patient and to prevent misunderstandings or doubts about best surgical practice and thereby avoid malpractice claims^[21,22]. In this context, it is worth exploring available peer review protections, such as the federal Patient Safety and Quality Improvement Act of 2005 in the United States, to provide additional safeguards around these recordings.

The ultimate goal is to promote a culture of error tolerance through a systematic review of recorded data. For example, the more errors that are exposed through routine recording, the better we will understand

what is considered within the real range of standard of care). Routine recording in the operating room has the potential to provide a tremendous long-term positive impact on surgical quality. Ensuring compliance with legal processes in these decisions requires the involvement of legal experts when designing pathways for routine recording.

Statement - Impact on medical malpractice claims

27. The availability of data from the operating room that in the past was not routinely recorded will directly improve operative patient care, particularly when used for quality improvement processes.

28. It is difficult and, in some cases, impossible to objectively and reliably interpret data originating from the operating room when used by either the plaintiff or the defendant for a potential malpractice claim.

29. It is important to assess whether specific data is discoverable and whether it should be part of medical records.

30. The involvement of legal experts when designing pathways for routine recording is imperative.

CONCLUSION

This manuscript describes several implementation barriers that need to be considered prior to designing an infrastructure for routine recording in the operating room at any institution. Given the absence of a comprehensive guide in the literature to summarize these barriers, a guide that outlines a path to implementation is needed. The 30 statements were agreed upon by all authors and represent the main points of the manuscript. Addressing these barriers will help reduce the risk associated with the task, but will not entirely avoid all risks. While some risk is unavoidable (ideally at a very low level), the benefit is expected to significantly outweigh such risk with the appropriate policies and processes in place. Hence, each institution needs to perform an individualized risk/benefit assessment [Table 2].

Prior to determining workflows and physically implementing routine recording, it is recommended to address all items listed on the checklist in Table 3. The checklist is not meant to be complete but to emphasize the most common barriers that need to be considered and adjusted to the local environment. It is also not intended to dictate policymaking.

Workflows of routine recording in the operating room typically benefit from standardization throughout the institution with similar processes for all services and all operating rooms. Given the need for operative care and non-clinical spaces (e.g., storage of data) to operate in sequence, interoperability has to be assessed and tested prior to implementation. The chosen process should undergo further testing for its usability. While the easiest solution is frequently the use of a commercially available, large-scale, unified platform supported by automation through AI systems, given the tremendous variabilities amongst jurisdictions, it is up to each institution to verify compliance and appropriate risk mitigation of such platforms (which usually requires a detailed understanding of the technology) and to assess whether the platform accommodates clinical practices and proposed processes. It is, therefore, sometimes necessary to consider less automated, local, and individual approaches. Such individual processes should be grounded in written institutional policies.

Once a process has been implemented, efforts cannot stop at recording. The ultimate dream would be for researchers to not only be able to record data in the operating room on a large scale, but to one day enable the data that is being recorded to be registered in a standardized fashion. Furthermore, for the collected data to have an impact, the information needs to be structured, annotated, analyzed, and subsequently utilized with the unified goal of improving clinical care through research, quality improvement, and/or education. AI plays an important role not only in allowing routine recording (e.g., auto-deidentification), but even more so in allowing integration of the resulting wealth of information into clinical practice.

Table 2. Perceived benefits and risks of routine data recording in the operating room

| Benefits | Risks |
|--|--|
| <ul style="list-style-type: none"> ● Research to improve healthcare ● Quality improvement/patient safety ● Education ● Expanded patient care/allowing for new approaches | <ul style="list-style-type: none"> ● Loss of privacy ● Unjust assumptions during malpractice claims ● Judgement of provider performance ● Financial cost ● Regulatory risk ● System pressures impacting patients', surgeons', and OR teams' autonomy |

Table 3. Checklist of requirements necessary for successful implementation of routine data recording in the operating room

| Topics that need to be addressed prior to implementing routine recording in the operating room |
|---|
| <p>Consent process</p> <ul style="list-style-type: none"> <input type="checkbox"/> Well-defined patient consent process (depending on the purpose for data recording), including an explanation about <ul style="list-style-type: none"> ● type of data to be recorded ● what the data will and will not capture ● handling and storage of the data ● scope of use of the data ● access to data and sharing of data ● associated risk and benefit ● alternative options <input type="checkbox"/> Exceptions of informed consent <ul style="list-style-type: none"> ● patients not competent to provide consent in the absence of proxy/guardian ● time-sensitive emergent operations ● voluntary waived consent <input type="checkbox"/> Consent process for emergent/urgent operations and vulnerable populations <input type="checkbox"/> Evaluation of whether data will be shared with patients <input type="checkbox"/> Conflict management of consenting provider <input type="checkbox"/> Implicit consent by surgeon and surgical team <input type="checkbox"/> Optout options by everyone involved <input type="checkbox"/> Handling of data if consent would be withdrawn in the future <input type="checkbox"/> More stringent process if data is not de-identified or coded <input type="checkbox"/> Solutions for increased workload associated with consent <p>Technical requirements</p> <ul style="list-style-type: none"> <input type="checkbox"/> Recording device that allows for collection of the required data within legal requirements, including features such as <ul style="list-style-type: none"> ● collecting digital raw data in its original format and uncorrupted state that conforms to computing ● domain-specific interconnectivity between devices ● cloud-based storage with adequate space and security ● automated features, such as recording, deidentification, and bookmarking ● real-time use, such as replay option <input type="checkbox"/> Transparent processes of data preparation <ul style="list-style-type: none"> ● curation of data and file naming ● deidentification or coding of data and metadata ● data annotation <input type="checkbox"/> Training of staff on the involved devices <input type="checkbox"/> Ability to stop automated recording if consent or other criteria are not met <p>Data use and access</p> <ul style="list-style-type: none"> <input type="checkbox"/> Intended use of recorded data, which will dictate regulatory pathways and processes <input type="checkbox"/> Who has access to the data, including the potential for patient access <input type="checkbox"/> Limitation of access on a need-to-know basis <input type="checkbox"/> Careful review of processes if third-party sharing (e.g., data donation) is involved <input type="checkbox"/> Assessment of whether vendors of involved devices have access to data <input type="checkbox"/> Secure systems for data sharing <input type="checkbox"/> Impact of sharing data on future intellectual property of licensing claims <input type="checkbox"/> Data use and access policy <p>Data privacy and security</p> <ul style="list-style-type: none"> <input type="checkbox"/> Impact of recording on privacy rights for patients and surgical team <input type="checkbox"/> Minimizing recording of identifiers and protected health information <input type="checkbox"/> Consent and data retention process need to address privacy concerns <input type="checkbox"/> Evaluate the need and the effectiveness of de-identification or coding of data <input type="checkbox"/> Adequacy of data security measures to meet industry standards <input type="checkbox"/> Minimization of data access <input type="checkbox"/> Maintenance plan to address future security threats <input type="checkbox"/> Data management policy |

Data retention

- ☐ Compliance with local regulatory rules
- ☐ Data maintenance/management plan
- ☐ Pre-defined duration of retention of protected health information vs. de-identified data
- ☐ Process of how any data is deleted, including previously shared data
- ☐ Need for data retention policy

Data ownership

- ☐ Identification of potential stakeholders given frequent legal ambiguity
- ☐ Clarification of responsibilities linked to ownership
- ☐ Potential contractual agreements amongst relevant stakeholders

Governance

- ☐ Identification of regulatory requirements and relevant stakeholders
- ☐ Process of handling sentinel event reviews
- ☐ Proactive surveillance of regulatory compliance
- ☐ Institutional oversight of user competence and training

Financial cost

- ☐ Identification of cost (fixed cost, operating cost, indirect cost, etc.)
- ☐ Identification of required funds
- ☐ Evaluate the potential for revenue
- ☐ Business plan

Impact on medical malpractice claims

- ☐ Impact on malpractice claims is uncertain and requires institutional assessment
 - ☐ Determination if specific data is discoverable and whether it should be part of medical records
 - ☐ Involvement of legal and compliance experts in the design phase
-

DECLARATIONS**Authors' contributions**

Made substantial contributions to the conception and design of the study and performed data analysis and interpretation: Schnelldorfer T, Gumbs AA, Grasso SV

Performed data acquisition, as well as providing administrative, technical, and material support: Schnelldorfer T, Gumbs AA, Tolkoff J, Choksi S, Stockheim J, Madani A, Pugh CM, Ishizawa T, Speidel S, Swanström LL, Rau BM, Szold A, Ausania F, Filicori F, Croner R, Grasso SV

Contributed to conceptualization, validation, review and editing: Schnelldorfer T, Gumbs AA, Tolkoff J, Choksi S, Stockheim J, Madani A, Pugh CM, Ishizawa T, Speidel S, Swanström LL, Rau BM, Szold A, Ausania F, Filicori F, Croner R, Grasso SV

Availability of data and materials

Not applicable.

Financial support and sponsorship

None.

Conflicts of interest

Gumbs AA is the Editor-in-Chief of *Artificial Intelligence Surgery* Journal. Schnelldorfer T, Pugh CM, Ishizawa T, Speidel S, Swanström LL, Rau BM, Szold A, Ausania F, Croner R and Grasso SV are the editorial board members of *Artificial Intelligence Surgery* Journal. Filicori F is a consultant for Boston scientific and receives research support from Intuitive Surgical. Other authors declared that there are no conflicts of interest. The Academic Editor Hengrui Liang will no longer serve as the journal's academic editor upon the expiration of his term in August 2024.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

© The Author(s) 2024.

REFERENCES

- Gumbs AA, Alexander F, Karcz K, et al. White paper: definitions of artificial intelligence and autonomous actions in clinical surgery. *Art Int Surg* 2022;2:93-100. DOI
- Maier-Hein L, Eisenmann M, Sarikaya D, et al. Surgical data science - from concepts toward clinical translation. *Med Image Anal* 2022;76:102306. DOI
- Levin M, McKechnie T, Kruse CC, Aldrich K, Grantcharov TP, Langerman A. Surgical data recording in the operating room: a systematic review of modalities and metrics. *Br J Surg* 2021;108:613-21. DOI
- Shah P, Thornton I, Turrin D, Hipkind JE. Informed consent. Available from: <https://www.ncbi.nlm.nih.gov/books/NBK430827/>. [Last accessed on 16 Jan 2023].
- Dalen ASHM, Legemaate J, Schlack WS, Legemate DA, Schijven MP. Legal perspectives on black box recording devices in the operating environment. *Br J Surg* 2019;106:1433-41. DOI
- Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: a novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS One* 2020;15:e0243043. DOI
- Madani A, Namazi B, Altieri MS, et al. Artificial intelligence for intraoperative guidance: using semantic segmentation to identify surgical anatomy during laparoscopic cholecystectomy. *Ann Surg* 2022;276:363-9. DOI
- Mascagni P, Alapatt D, Sestini L, et al. Computer vision in surgery: from potential to clinical value. *NPJ Digit Med* 2022;5:163. DOI
- Dimick JB, Scott JW. A video is worth a thousand operative notes. *JAMA Surg* 2019;154:389-90. DOI
- Shiroshita H, Inomata M, Akira S, et al. Current status of endoscopic surgery in Japan: the 15th National Survey of Endoscopic Surgery by the Japan Society for Endoscopic Surgery. *Asian J Endosc Surg* 2022;15:415-26. DOI
- Prigoff JG, Sherwin M, Divino CM. Ethical recommendations for video recording in the operating room. *Ann Surg* 2016;264:34-5. DOI
- D'Acquisto G, Domingo-Ferrer J, Kikiras P, Torra V, de Montjoye YA, Bourka A. Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. 2015. Available from: <https://doi.org/10.2824/641480>. [Last accessed on 16 Jan 2023]
- Filicori F, Addison P. Intellectual property and data ownership in the age of video recording in the operating room. *Surg Endosc* 2022;36:3772-4. DOI
- Li L, Fan Y, Tse M, Lin KY. A review of applications in federated learning. *Comput Ind Eng* 2020;149:106854. DOI
- Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. *IEEE Signal Process Mag* 2020;37:50-60. DOI
- Ahmadi SA, Sadat H, Scheufler KM, Steiger HJ, Weber B, Beez T. Malpractice claims in spine surgery in Germany: a 5-year analysis. *Spine J* 2019;19:1221-31. DOI
- Morton JM, Khoury H, Brethauer SA, et al. First report from the American Society of Metabolic and Bariatric Surgery closed-claims registry: prevalence, causes, and lessons learned from bariatric surgery medical malpractice claims. *Surg Obes Relat Dis* 2022;18:943-7. DOI
- Delaunay F, Delaunay T, Van Vyve E, Cardin JL; Club Coelio. Analysis of malpractice claims: the Franco-Belgian "Cœlio Club" experience. *J Visc Surg* 2019;156:S33-9. DOI
- De Ravin E, Sell EA, Newman JG, Rajasekaran K. Medical malpractice in robotic surgery: a Westlaw database analysis. *J Robot Surg* 2023;17:191-6. DOI
- Douglas RN, Stephens LS, Posner KL, et al. Communication failures contributing to patient injury in anaesthesia malpractice claims. *Br J Anaesth* 2021;127:470-8. DOI
- Humphrey KE, Sundberg M, Milliren CE, Graham DA, Landrigan CP. Frequency and nature of communication and handoff failures in medical malpractice claims. *J Patient Saf* 2022;18:130-7. DOI
- Levinson W, Roter DL, Mullooly JP, Dull VT, Frankel RM. Physician-patient communication. The relationship with malpractice claims among primary care physicians and surgeons. *JAMA* 1997;277:553-9. PubMed