npj | digital medicine

www.nature.com/npjdigitalmed

COMMENT OPEN

Check for updates

# Protecting procedural care—cybersecurity considerations for robotic surgery

William J. Gordon[1,2,3]✉, Naruhiko Ikoma[4], Heather Lyu[4], Gretchen Purcell Jackson[5,6] and Adam Landman[2,7]

Cybersecurity is an increasingly important concern for reliable healthcare delivery and is particularly salient for robotic surgery. Surgical robots are complex systems with numerous points of vulnerability, and there have been real-world demonstrations of successful cyberattacks on surgical robots. There are several ways to improve the risk profile of robotic surgery, including recognizing system complexity, investing in regular software updates, following cybersecurity best-practices, and increasing transparency for all stakeholders. As robotic surgery continues to technologically advance, ensuring overall system safety from a cybersecurity perspective is paramount.

*npj Digital Medicine* (2022)5:148 ; https://doi.org/10.1038/s41746-022-00693-8

## BACKGROUND

The digitization of care delivery has had a profound impact on nearly all facets of healthcare. However, an increasing reliance on technology has created new risks, and healthcare has not been immune to the cybersecurity considerations plaguing other industries. Cybersecurity attacks have disabled entire hospital networks, delayed surgeries, diverted ambulances, and had significant operational disruptions worldwide[1–3]. Unfortunately, cybersecurity concerns are only increasing—70% of hospitals indicated having been victim to a recent significant security incident[4].

Healthcare systems are uniquely vulnerable to cybersecurity attacks for several reasons. Health information is particularly valuable, creating financial incentive for attackers seeking patient data. Additionally, cybersecurity protection tends to be under-resourced by healthcare organizations, which are focused on care delivery and may have limited IT resources to spend on cybersecurity concerns. Finally, healthcare system attack surfaces are quite large. In addition to Electronic Health Records (EHRs), targets include hundreds and sometimes thousands of endpoints, such as patient devices (glucometers, pacemakers), hospital devices (infusion pumps, MRI scanners), medication dispensing systems, laboratory systems, anesthesia systems, to name only a few. Many devices are increasingly connected to the internet, creating further opportunities for attack. As an increasing public health concern[2], cybersecurity will only become more relevant in the years to come.

One healthcare setting that is becoming more digital is procedural care. Through the procedural care spectrum—pre-, peri-, and post-operative—clinicians are increasingly relying on digital and technological capabilities to improve, augment, or enable procedures and operations. The international recognition of the importance of healthcare information security has accelerated over the past five years, driven by real-world events causing significant care disruptions, but much of the focus has been on system resiliency—ensuring that the information systems that operate healthcare organizations remain functional and online. The perceived risks are around downtime and disruption. However, the cybersecurity risks posed to perioperative care are uniquely concerning because of the active nature of surgery—operative interventions have an immediate, physical impact on patients, creating the potential for significant physical harm if attacked[5]. In this commentary, we explore the cybersecurity considerations for delivering procedural care, with a focus on robotic surgery as a driving use case.

## ROBOTIC SURGERY: A USE-CASE FOR CYBERSECURITY CONSIDERATIONS OF PROCEDURAL CARE

Robotic surgery is a good use-case for exploring the cybersecurity considerations of procedural care. Surgical robotics, which enable a surgeon to control robotic arms within a patient from a console, has had increased adoption over the past several decades. More than a third of general surgeons performed robotic surgery in 2021, up from 8.7% in 2018 and this number is growing across other surgical specialties, including gynecology, urology, otolaryngology, and cardiothoracic surgery[6–8]. Complex operations such as those requiring vascular dissection and reconstruction are increasingly being performed robotically, and hospitals are adapting to incorporate robotic surgery to all surgical practices and training. Modern surgical robots are complex, multi-layered systems, with unique mechanical and software controls that enable more precise tissue handling and motion scaling than other minimally invasive techniques[9]. Robotic surgery offers numerous advantages compared to non-robotic minimally invasive surgery, including better field visualization, dexterity benefits, operator ergonomics, and in some cases, improved clinical outcomes compared to other techniques[10]. In addition, although not being performed in routine practice, there is a technological capability to allow surgeons to remotely control robots to operate on patients residing in underserved areas, which is considered a potential solution to mitigate geographic disparity in access to surgical care. Disadvantages of robotic surgery include potentially increased costs, longer duration of procedures, and inconclusive clinical benefits depending on the surgical indication[10,11].

[1]Department of Medicine, Brigham and Women's Hospital, Boston, MA, USA. [2]Mass General Brigham, Somerville, MA, USA. [3]Department of Biomedical Informatics, Harvard Medical School, Boston, MA, USA. [4]Department of Surgical Oncology, University of Texas MD Anderson Cancer Center, Houston, TX, USA. [5]Department of Pediatric Surgery, Pediatrics, Biomedical Informatics, Vanderbilt University Medical Center, Nashville, TN, USA. [6]Intuitive Surgical, Inc., Sunnyvale, CA, USA. [7]Department of Emergency Medicine, Brigham and Women's Hospital, Boston, MA, USA. ✉email: wjgordon@partners.org

## CYBERSECURITY RISKS OF ROBOTIC SURGERY

The overall technical complexity of robotic surgery systems creates unique cybersecurity risks and harms. A breach of a surgical robot, like any tool with direct patient contact, could lead to immediate and critical physical harm. Cybersecurity concerns about other devices, such as implantable cardiac pacemakers have received widespread attention[12]. This risk is not an unwarranted futuristic fear. In 2015, Bonaci and colleagues demonstrated the technical ability to take over control of robotic function in a simulated environment, disrupting and overriding robotic functions[13]. More recently, several vulnerabilities were discovered in robots used to deliver medical supplies in a hospital[14]. Systems that can cause direct harm need physical *and* non-physical controls to reduce risk.

Contemporary surgical robots are multifaceted mechanical and digital platforms that integrate data and deliver insights using advanced computational methodologies to augment the procedural experience. Some robotic systems offer advanced imaging features to aid in identification of anatomic structures and evaluation of vascular perfusion; others provide telemonitoring and telepresence capabilities to facilitate training and intraoperative consultation. The integration of data sources, hardware, software, and networking necessary to accomplish these functions introduces new vulnerabilities and might enable an attack that could scale to multiple robots simultaneously.

Artificial intelligence techniques such as machine learning are finding numerous applications in the robotic surgery, such as identification of anatomic structures or operative tasks, prediction of procedure time, and improving visual tissue differentiation[15–17]. Artificial intelligence solutions often require significant data for development and a technical infrastructure for operation, and their performance can change over time, introducing additional cybersecurity risks. Beyond advanced computational methodologies, surgical robotics is also dependent on many communication, informational, and basic network technologies to operate. Intraoperative vendor communication, for example, is often helpful for troubleshooting, but is reliant on networked connections to sites outside of the hospital firewalls. Surgical data logs and patient videos are also points of attack, and breaches could compromise confidential preference data, surgeon-specific performance information, or patients' personal health information. Robots are dependent on more general hospital infrastructure, like power, which could be interrupted. Robots require software updates and patches, which are points of vulnerability (e.g., through a man-in-the-middle or supply-chain attack, where the attacker may insert themselves between the robot and the server hosting the update software). Some robotic surgery platforms offer comprehensive subscription models that include cloud-based video recording hubs, performance tracking, and mobile access, all of which are further points of vulnerability. Finally, like other networked software devices, robotics could be compromised via physical means, become collateral damage from a wider attack, or fall victim to other traditional attacks, including deliberate employee misuse, denial of service attacks, or counterfeit equipment.

## STRATEGIES TO REDUCE CYBERSECURITY RISKS FOR ROBOTIC SURGERY

Fortunately, there are numerous ways to mitigate and improve risk profiles for robotic surgery. First, organizations need to recognize the complexity of surgical robotics and build cybersecurity practices around this complexity. For example, surgical robots include hardware, firmware, and software; each will have different risks and strategies to improve safety. Hardware concerns, for example, may involve close relationships with manufacturers to reduce the risk that individual components like field-programmable gate arrays have not been compromised[18]. From a software perspective, device manufacturers need to invest heavily in building software with security in mind, and regularly updating software. The Da Vinci robot, for example, has regular software updates[19]. Other surgically adjacent features of the robot—like vendor support functionality, training capabilities, and video recordings—also need consideration and cybersecurity optimization. It should be carefully considered to what extent a robotics platform needs real-time internet connectivity during a procedure as a further way to lower risk—separate, private networks could also reduce risk.

Second, organizations should follow general, best-practice cybersecurity hygiene, including data encryption, anti-virus software, employee training, and a risk-based approach to cybersecurity[2,20]. Mitigation strategies, such as training OR staff on emergency robotic undocking[21], threat identification, incident response planning are essential for preparedness. Individual employees remain the biggest organizational cybersecurity risk—it only takes one successful phishing campaign to elicit credentials that can give someone access to internal systems[22]. The US Food and Drug Administration (FDA) has published extensive pre-market and post-market documentation and guidance for device cybersecurity[23,24], as has the European Medicine Agency, the US National Institute for Standards and Technology, the International Medical Device Regulators Forum, and others. Aligning organizational posture with best-practice guidelines will never guarantee cybersecurity safety, but will mitigate risk, and provide defensibility should there be an attack.

Finally, transparency for providers and patients involved in surgical robotic care is critical. While the expectation is that increased automation and reliance on data will improve value as well as clinical outcomes, the dependencies created by a highly networked and data-intensive surgical robot should be called out, and appropriate downtime procedures are needed. A surgery could be delayed if the robot is not functioning but addressing an intraoperative performance degradation or outage is far more complex. Identifying these hazards in a transparent fashion will enable a realistic assessment of the probability of occurrence, and lead to better downtime procedures. Vendors and providers must work together to understand what the risks are and focus on continuously reducing those risks as the technology continues to mature and advance. Further, in the event of a cybersecurity incident, vendors should have procedures for promptly notifying providers with complete information, enabling provider organizations to understand the risks and mitigate appropriately. Organizations such as the Health Information Sharing and Analysis Center (H-ISAC), HHS Health Sector Cybersecurity Coordination Center (HC3), or a Patient Safety Organization[25] may help with communications.

## CONCLUSION

Robotic surgery is at the forefront of technology-driven care innovation. Like other areas of healthcare delivery that are increasingly dependent on technology, cybersecurity risk is an unfortunate reality. Cybersecurity concerns are particularly salient for robotic surgery because of the risk profile, which goes beyond merely downtime, and includes direct, physical patient harm. While these systems offer numerous advantages, there is an inherent vulnerability in any complex digital system. Understanding these risks while simultaneously working to reduce them will lead to safer and more reliable surgical care.

## DATA AVAILABILITY

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Received: 30 June 2022; Accepted: 1 September 2022;
Published online: 20 September 2022

## REFERENCES

1. Skahill, E. & West, D. Why hospitals and healthcare organizations need to take cybersecurity more seriously. https://www.brookings.edu/blog/techtank/2021/08/09/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/ (2021).
2. Gordon, W. J., Fairhall, A. & Landman, A. Threats to information security—public health implications. *N. Engl. J. Med.* **377**, 707–709 (2017).
3. Nigrin, D. J. When 'Hacktivists' target your hospital. *N. Engl. J. Med.* **371**, 393–395 (2014).
4. HIMSS. *2020 HIMSS Cybersecurity Survey*. https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf (HIMSS, 2020).
5. Fosch-Villaronga, E. & Mahler, T. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Comput. Law Secur. Rev.* **41**, 105528 (2021).
6. Sheetz, K. H., Claflin, J. & Dimick, J. B. Trends in the adoption of robotic surgery for common surgical procedures. *JAMA Netw. Open* **3**, e1918911 (2020).
7. Barbash, G. I. & Glied, S. A. New technology and health care costs–the case of robot-assisted surgery. *N. Engl. J. Med.* **363**, 701–704 (2010).
8. Stringfield, S. B. et al. Experience with 10 years of a robotic surgery program at an Academic Medical Center. *Surg. Endosc.* **36**, 1950–1960 (2022).
9. Thai, M. T. et al. Advanced intelligent systems for surgical robotics. *Adv. Intell. Syst.* **2**, 1900138 (2020).
10. Muaddi, H. et al. Clinical outcomes of robotic surgery compared to conventional surgical approaches (laparoscopic or open): a systematic overview of reviews. *Ann. Surg.* **273**, 467–473 (2021).
11. Gkegkes, I. D., Mamais, I. A. & Iavazzo, C. Robotics in general surgery: a systematic cost assessment. *J. Minimal Access Surg.* **13**, 243–255 (2017).
12. FDA. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (FDA, 2018).
13. Bonaci, T. et al. To make a robot secure: an experimental analysis of cyber security threats against teleoperated surgical robots. http://arxiv.org/abs/1504.04339 (2015).
14. Osborne, C. Critical vulnerabilities uncovered in hospital robots. *ZDNet* https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-medical-robots/ (2022).
15. Shvets, A. A., Rakhlin, A., Kalinin, A. A. & Iglovikov, V. I. Automatic Instrument Segmentation in Robot-Assisted Surgery using Deep Learning. in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)* 624–628. https://doi.org/10.1109/ICMLA.2018.00100 (2018).
16. Maier-Hein, L. et al. Surgical data science—from concepts toward clinical translation. *Med. Image Anal.* **76**, 102306 (2022).
17. Kassahun, Y. et al. Surgical robotics beyond enhanced dexterity instrumentation: a survey of machine learning techniques and their role in intelligent and autonomous surgical actions. *Int. J. Comput. Assist. Radiol. Surg.* **11**, 553–568 (2016).
18. Clark, G. W., Doran, M. V. & Andel, T. R. Cybersecurity issues in robotics. in *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)* 1–5. https://doi.org/10.1109/COGSIMA.2017.7929597 (2017).
19. Intuitive. *Da Vinci Software Integrating your da Vinci experience*. https://www.intuitive.com/en-us/products-and-services/da-vinci/software (2022).
20. Argaw, S. T. et al. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **20**, 146 (2020).
21. Melnyk, R. et al. Design and implementation of an emergency undocking curriculum for robotic surgery. *Simul. Healthc. J. Soc. Simul. Healthc.* **17**, 78–87 (2022).
22. Posey, C. & Shoss, M. *Research: Why Employees Violate Cybersecurity Policies*. (Harvard Business Review, 2022).
23. FDA. *Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Draft Guidance for Industry and Food and Drug Administration Staff*. https://www.fda.gov/media/119933/download (FDA, 2022).
24. FDA. *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*. https://www.fda.gov/media/95862/download (FDA, 2016).
25. HHS. *Understanding Patient Safety Confidentiality*. https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html (2022).

## ACKNOWLEDGEMENTS

The authors would like to thank Russel Berger for reviewing a final draft of this manuscript.

## AUTHOR CONTRIBUTIONS

W.J.G. drafted the manuscript. N.I., H.L., G.P.J., A.L. provided significant writing, reviewing, and editing of all versions.

## COMPETING INTERESTS

W.J.G. reports consulting income from Novocardia Inc., outside the scope of this article. W.J.G. reports no competing non-financial interests. G.P.J. is an employee of Intuitive Surgical, Inc. G.P.J. reports no competing non-financial interests. N.I. reports research support from Intuitive Surgical. H.L. reports no competing financial or non-financial interests. A.L. reports consulting income as a member of the Abbott Medical Device Cybersecurity Council. A.L. reports no competing non-financial interests.

## ADDITIONAL INFORMATION

**Correspondence** and requests for materials should be addressed to William J. Gordon.