1-4-2024

Video Endoscopy as Big Data: Balancing Privacy and Progress in Gastroenterology

Eugenia N. Uche-Anya
Harvard Medical School

Sara Gerke
Pennsylvania State Dickinson Law, sgerke@psu.edu

Tyler M. Berzin
Harvard Medical School

Open

Video Endoscopy as Big Data: Balancing Privacy and Progress in Gastroenterology

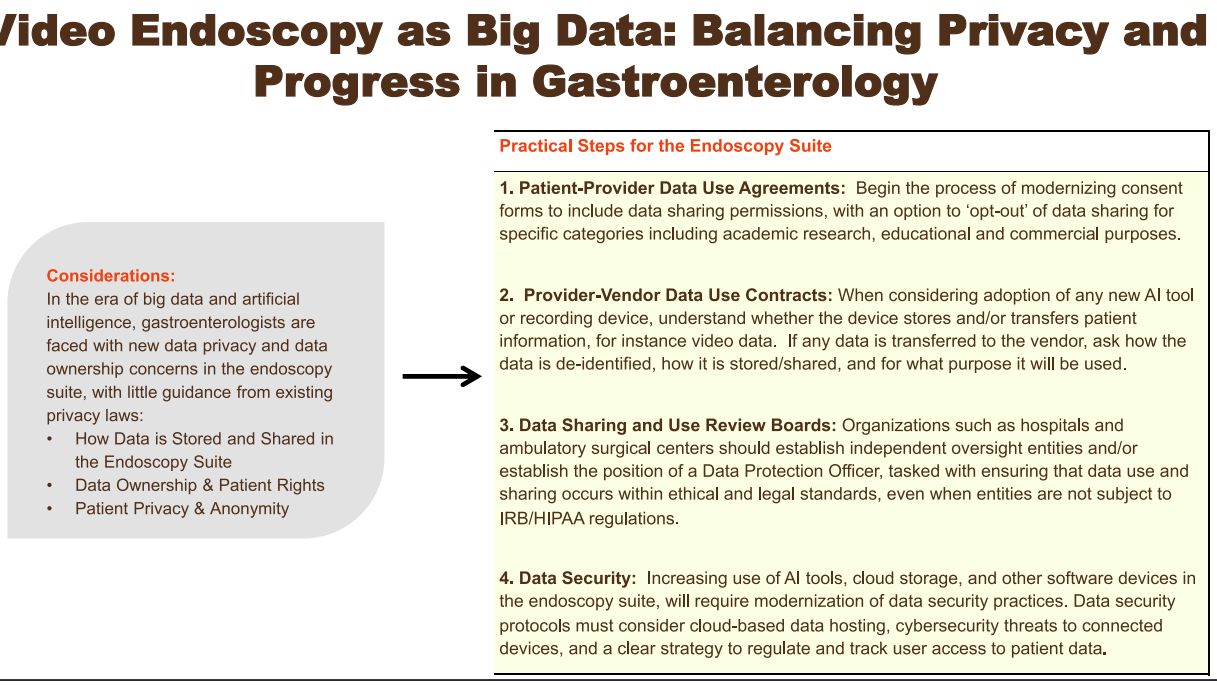
Eugenia N. Uche-Anya, MD, MPH[1], Sara Gerke, Dipl-Jur Univ, MA[2] and Tyler M. Berzin, MD, MS, FACG[3]

Am J Gastroenterol 2024;00:1–6. https://doi.org/10.14309/ajg.0000000000002597; published online January 4, 2024

INTRODUCTION

Tens of millions of gastrointestinal (GI) endoscopy videos and images are generated annually in the United States (1). A single 15-minute endoscopic procedure, recorded at 30 frames per second, generates approximately 27,000 high-definition images, representing a treasure trove of potential data. In the era of artificial intelligence (AI) and machine learning (ML), this data stream will not only fuel innovative and clinically impactful research in gastroenterology for both academic and commercial purposes, but also introduce ethical and legal concerns that merit consideration. Gastroenterologists are now faced with navigating new questions around data privacy and data ownership that have previously not been central to the endoscopy suite.

There is already a rapidly growing ecosystem of medical device and technology companies building platforms to leverage the value of video endoscopy data. For example, Medtronic's GI Genius (a computer-aided polyp detection system) has been developed on a database of more than 13 million colonoscopy images, Virgo (an endoscopy video storage and AI analysis platform) has amassed a database of more than 400,000 endoscopic videos, and Iterative Scopes has established agreements with numerous GI practices, ambulatory centers, and pharmaceutical companies to leverage video endoscopy data to streamline drug trial recruitment (2,3). Large image and video datasets are already being mined for a wide variety of GI applications, ranging from the development of new AI algorithms for lesion



[1]Division of Gastroenterology, Massachusetts General Hospital, Harvard Medical School, Boston, Massachusetts, USA; [2]Pennsylvania State Dickinson Law, Pennsylvania State University, Carlisle, Pennsylvania, USA; [3]Center for Advanced Endoscopy, Beth Israel Deaconess Medical Center, Harvard Medical School, Boston, Massachusetts, USA. **Correspondence:** Eugenia N. Uche-Anya, MD, MPH. E-mail: eucheanya@mgh.harvard.edu.
Received July 1, 2023; accepted November 3, 2023

detection during endoscopic procedures to an array of digital tools that will support large scale, industry sponsored drug trials (particularly in the field of inflammatory bowel disease), facilitate patient recruitment and automate assessments of disease activity and treatment response.

The opportunity for critical advances in clinical care offered by the big data and AI/ML revolution in GI endoscopy must be balanced against important considerations regarding patient privacy and data ownership. Over the course of the next several years, hospitals, GI division leaders, and clinical researchers will be faced with important decisions around how to integrate digital tools in the endoscopy suite. In an era where "data is the new oil" (4), the GI endoscopy unit is a relatively untapped reserve, and gastroenterology leaders must be responsible stewards of this valuable resource. Our aim in this article is to provide a practical overview and guide for how gastroenterologists should navigate this new landscape, considering key ethical, legal, and professional considerations.

HOW ARE DATA STORED AND SHARED IN THE ENDOSCOPY SUITE?

The digital devices and software that may be installed in the endoscopy suite generally fall into one of several key categories. The first category is Software as a Medical Device (SaMD), which refers to standalone software that is designed to independently perform, or to help a human perform, a specific medical task (diagnosis, treatment, etc.) (5) SaMDs are classified as medical devices under the US Federal Food, Drug, and Cosmetic Act and are regulated by the US Food and Drug Administration (FDA). SaMDs are of central interest to the era of AI/ML and big data in medicine, and an increasing number of SaMD tools are already leveraging AI algorithms for clinical care. For instance, computer-aided detection (CADe) is an example of an SaMD; several colonic polyp CADe systems (6,7) have already received US FDA marketing authorization for use in clinical endoscopic practice. Critically, SaMDs may or may not store or transfer patient data, and gastroenterologists must be aware of their specific functionality to properly assess whether adoption of a particular SaMD raises specific legal or ethical considerations. In this regard, it is also important to understand that the US FDA is responsible for assessing the safety and effectiveness of SaMDs, but the agency is not the gatekeeper of data privacy.

A second category of software in the endoscopy suite comprises electronic health record (EHR) platforms, which, perhaps surprisingly, are not currently considered medical devices (8). The dividing line between EHRs and SaMDs may become increasingly gray as AI-supported decision tools become embedded in many EHR. Beyond the EHR, there is an ecosystem of other digital products and software tools in the endoscopy suite, which also fall outside the category of medical devices. For instance, software that enables cloud storage of endoscopy videos is not formally categorized as SaMD because it does not serve a direct clinical function (8,9) and instead may be used for research, education, or quality improvement purposes. The complexity around whether a software represents an SaMD is perhaps best exemplified by the fact that the Picture Archiving and Communication System, which stores and sends images in radiology departments, is not considered a medical device but the Picture Archiving and Communication System *viewer* software is because the physician interacts with the viewer more directly during medical care (10). Software in a Medical Device is a third category of software that does not stand alone but is embedded in a medical device (5), such as a software used to run a magnetic resonance imaging machine (11).

Whether an SaMD or digital product in the endoscopy suite *stores or transfers patient information* is a critical consideration and should be a focus of queries to any potential vendor. Examples of SaMDs that do not store or transfer data are current CADe platforms (e.g., Micro-Tech EndoScreener and Medtronic GI Genius). In their current iterations, the video data from the endoscopy processor are sent directly to a Graphics Processing Unit hardware installed locally in each endoscopy room. Data are analyzed by a polyp detection algorithm, and the output (a polyp detection alert box) is overlayed on a video stream sent in real time to the endoscopy monitor. At no point in this process is the video image stored on the Graphics Processing Unit nor sent through an internet connection to any other location. The vendors, in this case Micro-Tech or Medtronic, have no practical access to any clinical data. The contracts with these and similar digital product vendors should generally specify that no patient data will be stored or used by the vendor.

There is an increasing number of digital tools in the endoscopy suite, for which storage and transfer of patient data are materially central to the function and value proposition of the vendor's software tool. For instance, Virgo currently offers a cloud-based video storage platform for GI endoscopy units with flexible pricing plans (12). For gastroenterologists, this platform is intended to support recording of cases for teaching, research, and quality improvement purposes. In addition, the Virgo platform is promoted as a tool that may support and accelerate clinical trial recruitment by helping clinical researchers identify patients with specific diseases (for instance, Crohn's disease and ulcerative colitis) matching the criteria for entry into specific clinical trials. A publicly available example of the user agreement provides Virgo with a "royalty-free, perpetual, irrevocable, worldwide, royalty-free [sic], nonexclusive, and fully sublicensable right to use and license to use, license, distribute, reproduce, modify, and adapt Your Content" for their business purposes (13). This raises important questions regarding how patient data should be shared and used and what steps can be taken to maximize transparency for all involved parties.

DATA OWNERSHIP AND PATIENT RIGHTS

Who owns endoscopy-generated data? Certainly, under the Health Insurance Portability and Accountability Act (HIPAA), patients have rights to privacy, confidentiality, and security over their identifiable health information throughout the United States (14). However, in all states but New Hampshire (15), patients do *not* have explicit ownership rights to their health data; in several states, health providers do, while in others, there are no specific laws delineating health data ownership rights (16). Further complicating the picture is that legal precedence exists for not recognizing property rights over health information because it is a public good: this means that *no one* can own health data (17). The surprising reality is that patients have limited control over how their health data are used and shared. For example, covered entities under HIPAA—that is, most health providers, plans, and clearinghouses—are permitted to use individually identifiable health information without patient authorization for research purposes if ethical and regulatory stipulations set by the Institutional Review Board (IRB) are met

(18). Once health information is deidentified, health data can also be used with literally no restrictions and can even be shared with third parties that are not subject to HIPAA's requirements or IRB oversight.

There is a growing number of companies (19) focused on aggregating and monetizing large sets of health data for (sometimes undetermined) secondary uses that could be potentially exploitative. For example, an endoscopy-generated data-driven algorithm that predicts which healthy individuals will develop inflammatory bowel disease in the future can conceivably be discriminatorily used in determining insurance premiums or hiring decisions: similar practices have already occurred (20,21). As health data become increasingly commodified, it becomes apparent that there are gaps in existing laws intended to protect patients and secure good data stewardship.

In California, there are some efforts to diminish these gaps. The California Consumer Privacy Act grants California residents several rights, including the right to know whether collected information is being shared or sold (22). Eleven other states have also recently passed new privacy laws, but while those initiatives are a step in the right direction, they all have the same flaw in that they are limited in scope and exclusively apply to the state's residents (23,24). Without a comprehensive federal privacy law (or alternatively, all 50 states passing new privacy laws), not everyone's privacy in the United States will be properly protected. In comparison, the European Union's General Data Protection Regulation (GDPR) is more robust because it applies to all personal data and only allows the processing of health data under specific exceptions (such as explicit patient consent or scientific research purposes) (25).

PRIVACY AND ANONYMITY

Although HIPAA aims to protect individuals' health information, deidentification of health information—either by removing all 18 specified individual identifiers (such as names, zip codes, and phone numbers) or by having an expert determine that the risk of the anticipated recipient identifying an individual is small—exempts covered entities from HIPAA's privacy safeguards (26). However, deidentification of health information is becoming less and less sufficient for protecting patient privacy because data triangulation by linkage with diverse data sources can make reidentification possible. In addition, health data are now being generated from nontraditional sources such as apps and smartwatches by noncovered entities such as Google, Apple, and Amazon that are usually not subject to HIPAA (24,27). In the world of GI endoscopy, for instance, it is plausible that data from existing bowel preparation apps with associated email addresses and data from a deidentified endoscopy video storage platform could be linked and allow for reidentification of patients. Furthermore, GI endoscopy videos may sometimes include images of the patient's face or other identifying features, and while some companies/platforms promise automated video deidentification, including deletion of any video portions before or after scope insertion/withdrawal, some risk remains. Multiple reidentification efforts using deidentified health information have been well documented in the literature (28), thus illustrating HIPAA's limitations in protecting patient privacy as big data continue to expand. This also opens up the potential for litigation: in *Dinerstein v. Google* (29,30), the University of Chicago was accused of sharing identifiable health information with Google to develop an algorithm that predicts clinical outcomes for hospitalized patients (31). While the University of Chicago asserted that health information was deidentified in compliance with the HIPAA, the plaintiff claimed that with the dates of service and free text notes provided and Google's prolific data mining expertise, reidentification of almost every medical record shared was easily possible (29).

By contrast, the European Union's GDPR offers some clarity by using the term "anonymous information" rather than deidentification. The term "anonymous information" is stricter than its US counterpart, such that deidentified health information under HIPAA may be considered personal data under the GDPR and thus subject to its requirements (32,33). Anonymized data are not subject to GDPR requirements and can be used without restrictions (25). However, it is not clear how truly attainable anonymization of health information is in the current big data landscape, where data triangulation is progressively being simplified.

PRACTICAL STEPS FOR THE ENDOSCOPY SUITE

This decade represents a critical crossroads in the field of gastroenterology: we are on the brink of leveraging big data opportunities for GI endoscopy, while laws on patient privacy and data ownership are still very much evolving. So, what can gastroenterologists, directors of endoscopy, and practice/hospital leaders do to ensure that reasonable ethical and legal decisions are being made regarding patient data? We propose 4 recommendations that can be used as a starting point for this important discussion (Table 1).

Recommendation 1 (patient-provider data use agreements)

GI endoscopy consent forms could be modernized to include a brief data use agreement with the patient. The agreement could specify the extent of data collection, who is authorized to access the data (including third-party or commercial partners), and current and possible future uses (both known and unknown) of the data collected (Figure 1) (34). Compared with a specific consent model, a broad consent model is advantageous in that it strikes a balance between providing patients with initial control over their data without severely limiting the advances made possible by big data (27,35). However, the disadvantage is that patients usually no longer have control over their data once they sign the agreement. Because the conception of privacy is contextual, this could be problematic in certain cases, depending on who accesses the data and for what purposes specifically (27). To avoid misuse of patient data, some safeguards need to exist when using a broad consent model. Thus, we propose a tiered approach with 2 specific safeguards.

First, when technically feasible, patients should have the option to opt out of data use/sharing across specific categories, including academic research, educational purposes, and/or commercial purposes. This ability to opt out should be made easily available to patients at any point in time. This approach would also require always on video recording platforms to incorporate a privacy button, which temporarily turns off video recording for research or commercial purposes based on patient preference. Irrespective of whether the law requires it, clear and open disclosure of how patient data may be used is best practice because it promotes transparency and reinforces patient autonomy, which in turn cultivates patient trust and willingness to participate in data sharing. Sample wording for GI endoscopy consent that includes a tiered data use agreement with the patient

Table 1. Practical steps for the endoscopy suite

1. Patient-Provider Data Use Agreements: Begin the process of modernizing consent forms to include data sharing permissions, with an option to opt out of data sharing for specific categories including academic research, educational purposes, and commercial purposes
2. Provider-Vendor Data Use Contracts: When considering adoption of any new AI tool or recording device, understand whether the device stores and/or transfers patient information, for instance, video data. If any data are transferred to the vendor, ask how the data are deidentified, how they are stored/shared, and for what purpose they will be used
3. Data Sharing and Use Review Boards: Organizations such as hospitals and ambulatory surgical centers should establish independent oversight entities and/or establish the position of a Data Protection Officer, tasked with ensuring that data use and sharing occurs within ethical and legal standards, even when entities are not subject to IRB/HIPAA regulations
4. Data Security: Increasing use of AI tools, cloud storage, and other software devices in the endoscopy suite will require modernization of data security practices. Data security protocols must consider cloud-based data hosting, cybersecurity threats to connected devices, and a clear strategy to regulate and track user access to patient data

is shown in Figure 2 (36). We expect that approaches to patient consent will rapidly evolve in the next decade, with growing efforts to consider health literacy and patient preference in these complex discussions of big data.

Second, after the data use agreement is signed, there should be a Data Use and Sharing Review Board, which serves as the gatekeeper of patient privacy and protects patients from misuse of their data (see Recommendation 3).

Recommendation 2 (provider-vendor data use contracts)

Contracts with vendors offering an SaMD or any software tool in the endoscopy suite should clearly and exhaustively incorporate stipulations on how patient data are to be collected, stored, used, and shared. This includes delineating the type of data in question (videos, images, clinical diagnoses, etc), determining the extent of vendors' obligations and liabilities in securing patient data, and defining and specifying limits on vendors' rights to own, collect, and control access to, use, reuse, share, reidentify, aggregate, or sell patient data (deidentified or otherwise) (37,38). Conditions for contract termination and the extent of vendors' rights to previously accessed data in that setting should also be established (37). Regardless of the approach taken by the vendor, the intended use for patient data should be clearly delineated and made a central aspect of the contractual negotiation, recognizing that clinical data may be of very high commercial value to the vendor. Particular caution should be exercised when vendors offer their services or tools for free—this should perhaps encourage even heavier scrutiny and rigor on the contract policies with the vendors. Generally, it is best practice not to grant vendors more rights than are necessary to perform the services being offered (38). At the very least, requesting contractual terms prohibiting attempts at reidentification through linkage with other datasets or otherwise is advisable. The American College of Radiology has developed a sample provider-vendor data sharing contract, which is a great starting point and could be easily adapted to GI endoscopy (37). It is likely these provider-vendor contracts will need to evolve in the future to meet new needs that could potentially arise as the big data landscape continues to rapidly advance.

Recommendation 3 (data use and sharing review boards)

Data Use and Sharing Review Boards are independent oversight entities for data governance and stewardship, which ensure that data use and sharing—especially by entities not subject to IRB and HIPAA regulations—fall within the ethical standards discussed earlier (27,39,40). Similar to the IRB, these boards can approve or deny requests for data use or sharing if projects fail to meet ethical and legal guidelines or applicable laws, (41) and should have appropriate representation for patients, health providers, data privacy experts, and ethicists. Of note in Europe, the GDPR requires certain institutions that process personal data (including health data) to appoint a Data Protection Officer whose primary role is to independently oversee data privacy and protection in compliance with the GDPR (42,43). While not legally required in the United States, adopting a similar approach, either by expanding the role of the IRB in universities and public institutions, appointing Data Protection Officers, or creating Data Use and Sharing Review Boards in public and private settings, would be best practice in safeguarding patient privacy (27,39,40).

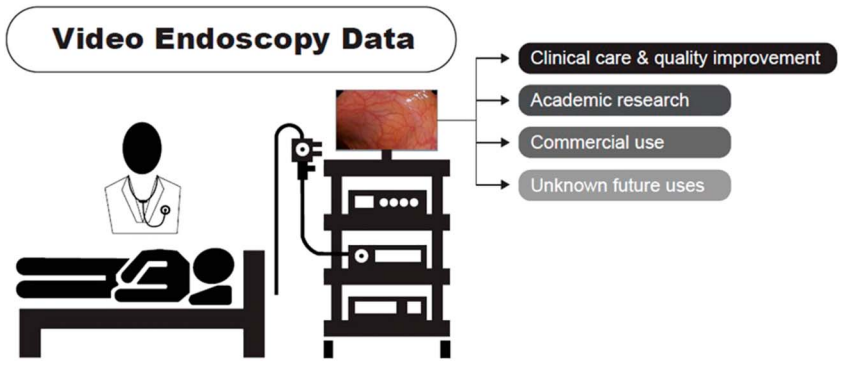


Figure 1. Potential uses of video endoscopy data (illustration by Danielle Duffey).

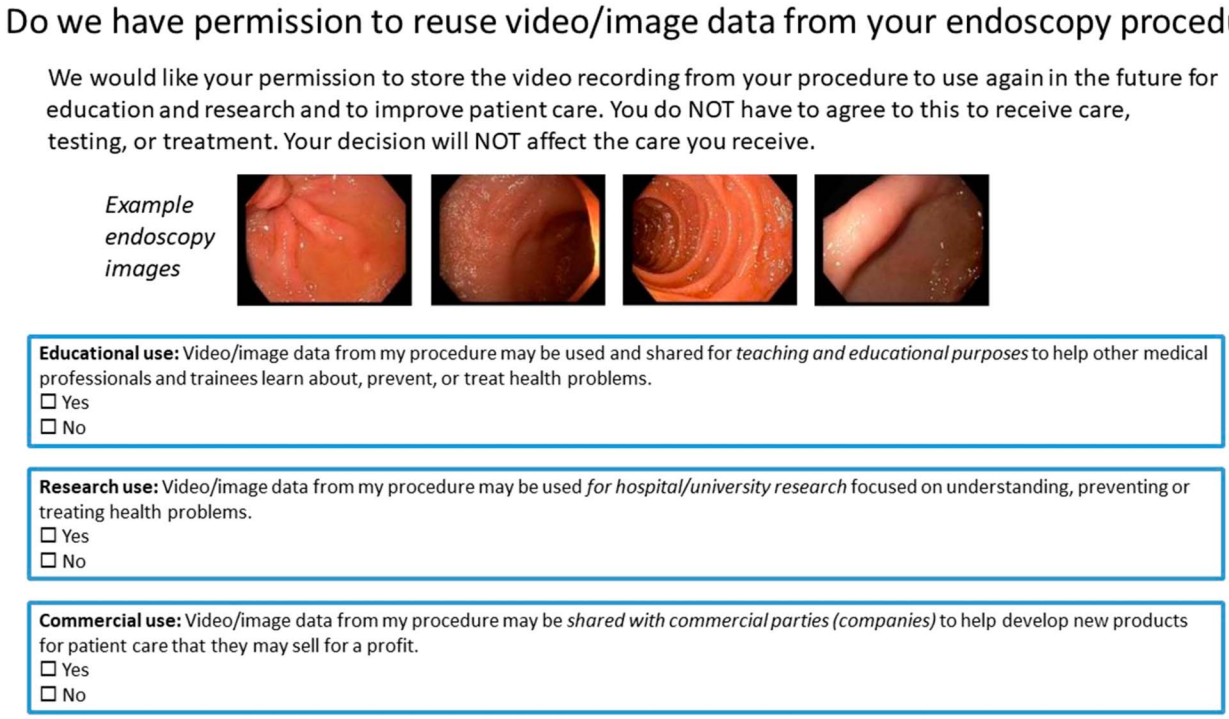


Figure 2. Sample tiered data use agreement for use of video/image data in GI endoscopy (adapted from Kotsenas et al) (36).

Recommendation 4 (data security)

Securing patient data is a challenging yet critical stakeholder responsibility, especially in the context of rising cybersecurity attacks and threats (38,44). Health providers, practices, and vendors should rigorously implement data security best practices and follow applicable laws (45) to protect patient data from unauthorized access or use and limit the hefty penalties associated with data breaches (14,44). Clear documentation of accountability for this task should be included in vendor contracts (see Recommendation 2), with particular attention paid to how the configuration and execution of a software tool may aid or deter data security. A third-party cloud-based tool, for example, could be seen as more susceptible to cybersecurity threats compared with tools hosted on in-house servers; this should be taken into consideration when developing and implementing data security protocols (38). Other recommended strategies for protecting patient data include restricting users' access to sensitive data on a need-to-know basis, securing data access with multifactor authentication and data encryption, and logging all data access and use for periodic security audits (46). Access from connected devices such as mobile phones, apps, and wearable devices are data security vulnerability points that can be disabled if nonessential or otherwise limited to the minimum necessary, encrypted and closely monitored (44,46). Regular data security risk assessments and policy reviews are advised to not only ensure that rapidly evolving cybersecurity standards are being met but also to proactively identify and strengthen areas of data security concerns (46). In addition, routine education (14) of data users on data security policies and equipping them with tools for detecting and avoiding threats such as phishing emails, scams, and malware can help foster a culture where data users are invested in maintaining data security.

CONCLUSION

In the era of big data and AI, gastroenterologists are faced with new data privacy and data ownership concerns in the endoscopy suite, with little guidance from existing privacy laws. This era will not only require new models of patient consent for data use and sharing, but gastroenterologists, practices, and hospitals must also become increasingly prepared to deal with vendor data use contracts for GI endoscopy as the value of endoscopy video data becomes increasingly important to commercial entities. Even as we wait for lawmakers to improve data protection in the United States, gastroenterologists should take a proactive approach by implementing best practices that promote transparency and patient autonomy during this critical moment of innovation and opportunity in the field.

CONFLICTS OF INTEREST

Guarantor of the article: Eugenia N. Uche-Anya, MD, MPH.
Specific author contributions: E.U., S.G. and T.M.B.: involved in project conception, literature review and interpretation, drafting the manuscript, and reviewing the manuscript critically for important intellectual content. All authors have approved the final submitted draft.
Financial Support: None to report.
Potential competing interests: Work conducted by S.G. and T.M.B. was funded by the European Union (Grant Agreement no. 101057099). Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. S.G. also reports grants from the European Union (Grant Agreement no. 101057321), the

National Institute of Biomedical Imaging and Bioengineering (NIBIB) and the National Institutes of Health Office of the Director (NIH OD) (Grant Agreement no. 3R01EB027650-03S1 and no. 1R21EB035474-01), and the National Institute on Drug Abuse (NIDA)/National Institutes of Health (NIH) (Grant Agreement no. 1U54DA058271-01). T.M.B. is a consultant for Medtronic, Wision AI, Microtech, Magentiq Eye, RSIP Vision, and Boston Scientific.

REFERENCES

1. Peery AF, Crockett SD, Murphy CC, et al. Burden and cost of gastrointestinal, liver, and pancreatic diseases in the United States: Update 2021. Gastroenterology 2022;162(2):621–44.
2. GI Genius Intelligent Endoscopy Module Brochure (https://www.medtronic.com/content/dam/medtronic-com/c/digestive-gastrointestinal/documents/gi-genius-brochure.pdf) (2021). Accessed April 25, 2023.
3. Olympus Corporation. Olympus innovation ventures backs endoscopy video and AI company, virgo surgical video solutions (https://www.prnewswire.com/news-releases/olympus-innovation-ventures-backs-endoscopy-video-and-ai-company-virgo-surgical-video-solutions-301594359.html). Accessed April 25, 2023.
4. Agrawal A, Gans J, Goldfarb A. Prediction Machines: The Simple Economics of Artificial Intelligence. Harvard Business Press: Brighton, MA, 2018.
5. United States Food and Drug Administration. Software as a medical device (SaMD). FDA (https://www.fda.gov/medical-devices/digital-health-center-excellence/software-medical-device-samd) (2020). Accessed June 9, 2023.
6. Chengdu Wision Medical Device Co., LTD. 510(k) premarket notification: EndoScreener (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/pmn.cfm?ID=K211326). Accessed June 9, 2023.
7. Cosmo artificial intelligence–AI ltd, riverside Cosmo artificial intelligence–AI ltd. 510(k) premarket notification: GI genius (https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfpmn/pmn.cfm?ID=K211951). Accessed June 9, 2023.
8. U.S. Federal Food, Drug and Cosmetic Act, 21 U.S.C. Chapter 9 § 520(1c) (https://www.fda.gov/media/109622/download). Accessed June 9, 2023.
9. U.S. Federal Food, Drug and Cosmetic Act, 21 U.S.C. Chapter 9 § 321(h) (https://www.govinfo.gov/content/pkg/COMPS-973/pdf/COMPS-973.pdf). Accessed June 26, 2023.
10. United States Food and Drug Administration. Medical devices; medical device classification regulations to conform to medical software provisions in the 21st century cures act. Federal Register (https://www.federalregister.gov/documents/2021/04/19/2021-07860/medical-devices-medical-device-classification-regulations-to-conform-to-medical-software-provisions) (2021). Accessed June 26, 2023.
11. Software as a medical device (SAMD)–classification overview (https://www.rimsys.io/blog/software-as-a-medical-device-samd). Accessed June 26, 2023.
12. FAQ frequently asked questions|A.I. for gastroenterology. Virgo (https://www.virgosvs.com/gi-resources/endoscopy-faq/). Accessed June 26, 2023.
13. Terms of use & privacy policy. Virgo (https://www.virgosvs.com/tos/). Accessed April 25, 2023.
14. US Department of Health and Human Services. "HIPAA administrative simplification: Regulation text, 45 CFR parts 160, 162, and 164." 2013 (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf) (2013). Accessed July 1, 2023.
15. N.H. Rev. Stat. Ann. § 151:21. Patients' Bill of Rights.
16. Who owns medical records: 50 state comparison|health information & the law (http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison). Accessed April 25, 2023.
17. Contreras JL. Genetic property. Georgetown L J 2016;105(1):1–54.
18. U.S. Department of Health and Human Services. Summary of the Hipaa Privacy Rule. Office for Civil Rights, 2003 (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf) (2003). Accessed June 26, 2023.
19. Tanner A. For sale: Your medical records. Scientific Am 2016;314(2):26–7.
20. Moody GA, Mayberry JF. Life insurance and inflammatory bowel disease: Is there discrimination against patients? Int J Colorectal Dis 1996;11(6):276–8.
21. Roberts JL. Healthism and the law of employment discrimination. Iowa L Rev 2013;99(2):571–636.
22. California Consumer Privacy Act (CCPA). State of California–Department of Justice–Office of the Attorney General (https://oag.ca.gov/privacy/ccpa) (2018). Accessed April 29, 2023.
23. International Association of Privacy Professionals. US state privacy legislation tracker (https://iapp.org/resources/article/us-state-privacy-legislation-tracker/). Accessed June 26, 2023.
24. Gerke S, Rezaeikhonakdar D. Privacy aspects of direct-to-consumer artificial intelligence/machine learning health apps. Intell Based Med 2022;6:100061.
25. General data protection regulation (GDPR) compliance guidelines. GDPR.eu (https://gdpr.eu/). Accessed April 29, 2023.
26. 45 C.F.R. § 164.514(a) and (b) (https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.514). Accessed June 26, 2023.
27. Price WN, Cohen IG. Privacy in the age of medical big data. Nat Med 2019;25(1):37–43.
28. Henriksen-Bulmer J, Jeary S. Re-identification attacks—a systematic literature review. Int J Inf Manag 2016;36(6):1184–92.
29. Dinerstein v. Google, LLC et al, No. 1:2019cv04311–Document 85 (N.D. Ill. 2020). Justia Law (https://law.justia.com/cases/federal/district-courts/illinois/ilndce/1:2019cv04311/366172/85/). Accessed April 29, 2023.
30. Dinerstein v. Google, LLC, No. 20-3134 (https://media.ca7.uscourts.gov/cgi-bin/OpinionsWeb/processWebInputExternal.pl?Submit=Display&Path=Y2023/D07-11/C:20-3134:J:Sykes:aut:T:fnOp:N:3073598:S:0). Accessed September 30, 2023.
31. Rajkomar A, Oren E, Chen K, et al. Scalable and accurate deep learning with electronic health records. NPJ Digit Med 2018;1:18.
32. Recital 26–general data protection regulation (GDPR). GDPR.eu (https://gdpr.eu/recital-26-not-applicable-to-anonymous-data/) (2018). Accessed June 26, 2023.
33. Gerke S. Privacy laws in the USA, Europe, and South Africa. In: AI in Clinical Medicine. John Wiley & Sons, Ltd, 2023, pp 395–406.
34. Lam K, Abràmoff MD, Balibrea JM, et al. A Delphi consensus statement for digital surgery. Npj Digit Med 2022;5(1):100–9.
35. Grady C, Eckstein L, Berkman B, et al. Broad consent for research with biological samples: Workshop conclusions. Am J Bioeth AJOB 2015;15(9):34–42.
36. Kotsenas AL, Balthazar P, Andrews D, et al. Rethinking patient consent in the era of artificial intelligence and big data. J Am Coll Radiol 2021;18(1 Pt B):180–4.
37. Batlle JC, Dreyer K, Allen B, et al. Data sharing of imaging in an evolving health care world: Report of the ACR data sharing workgroup, part 2: Annotation, curation, and contracting. J Am Coll Radiol JACR 2021;18(12):1655–65.
38. The Office of the National Coordinator for Health Information Technology. EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print (https://www.healthit.gov/sites/default/files/EHR_Contracts_Untangled.pdf). Accessed June 9, 2023.
39. Cohen IG, Mello MM. Big data, big tech, and protecting patient privacy. JAMA 2019;322(12):1141–2.
40. Parasidis E, Pike E, McGraw D. A Belmont report for health data. N Engl J Med 2019;380(16):1493–5.
41. Larson DB, Magnus DC, Lungren MP, et al. Ethics of using and sharing clinical imaging data for artificial intelligence: A proposed framework. Radiology 2020;295(3):675–82.
42. Article 37–general data protection regulation (GDPR). GDPR.eu (https://gdpr.eu/article-37-designation-of-the-data-protection-officer/) (2018). Accessed June 26, 2023.
43. Article 39–general data protection regulation (GDPR). GDPR.eu (https://gdpr.eu/article-39-tasks-of-the-data-protection-officer/) (2018). Accessed July 1, 2023.
44. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: Insights and implications. Healthcare 2020;8(2):133.
45. Office for Civil Rights. Summary of the HIPAA security rule. HHS.gov (https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html) (2009). Accessed September 30, 2023.
46. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: Preserving security and privacy. J Big Data 2018;5(1):1.