OPINIONS OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS

The following opinions were presented by David A. Fleming, MD, Chair:

1. RESPONSIBILITIES TO PROMOTE EQUITABLE CARE

CEJA Opinion; no reference committee hearing.

HOUSE ACTION: FILED

At the 2023 Annual Meeting, the American Medical Association House of Delegates adopted the recommendations of Council on Ethical and Judicial Affairs Report 4-A-23, "Responsibilities to Promote Equitable Care." The Council issues this Opinion, which will appear in the next version of AMA PolicyFinder and the next print edition of the *Code of Medical Ethics*.

E-11.2.7 – Responsibilities to Promote Equitable Care

Medicine at its core is a moral activity rooted in the encounter between a patient who is ill and a physician who professes to heal. The "covenant of trust" established in that encounter binds physicians in a duty of fidelity to patients. As witness to how public policies ultimately affect the lives of sick persons, physicians' duty of fidelity also encompasses a responsibility to recognize and address how the policies and practices of the institutions within which physicians work shape patients' experience of health, illness, and care. As the physical and social settings of medical practice, hospitals and other health care institutions share the duty of fidelity and, with physicians, have a responsibility to ensure that the care patients receive is safe, effective, patient centered, timely, efficient, and equitable.

Enduring health disparities across patient populations challenge these duties of fidelity. Disparities reflect the habits and practices of individual clinicians and the policies and decisions of individual health care institutions, as well as deeply embedded, historically rooted socioeconomic and political dynamics. Neither individual physicians nor health care institutions can entirely resolve the problems of discrimination and inequity that underlie health disparities, but they can and must accept responsibility to be agents for change.

In their individual practice, physicians have an ethical responsibility to address barriers to equitable care that arise in their interactions with patients and staff. They should:

(a) Cultivate self-awareness and strategies for change, for example, by taking advantage of training and other resources to recognize and address implicit bias;

(b) Recognize and avoid using language that stigmatizes or demeans patients in face-to-face interactions and entries in the medical record;

(c) Use the social history to capture information about non-medical factors that affect a patient's health status and access to care to inform their relationships with patients and the care they provide.

Within their institutions, as professionals with unique knowledge, skill, experience, and status, physicians should collaborate with colleagues to promote change. They should:

(d) Support one another in creating opportunities for critical reflection across the institution;

(e) Identify institutional policies and practices that perpetuate or create barriers to equitable care;

(f) Participate in designing and supporting well-considered strategies for change to ensure equitable care for all.

As institutions in and through which health care occurs, hospitals and other health care institutions share medicine's core values and commitment of fidelity, and with it ethical responsibility to promote equitable care for all. Moreover, as entities that occupy positions of power and privilege within their communities, health care institutions are uniquely positioned to be agents for change. They should:

(g) Support efforts within the institution to identify and change institutional policies and practices that may perpetuate or create barriers to equitable care;

(h) Engage stakeholders to understand the histories of the communities they serve and recognize local drivers of inequities in health and health care;

(i) Identify opportunities and adopt strategies to leverage their status within the community to minimize conditions of living that contribute to adverse health status. (I, VII, VII, IX)

REPORTS OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS

The following reports were presented by David A. Fleming, MD, Chair:

1. PHYSICIANS' USE OF SOCIAL MEDIA FOR PROUCT PROMOTION AND COMPENSATION

Reference committee hearing: see report of Reference Committee on Amendments to Constitution and Bylaws.

HOUSE ACTION: REFERRED

At its 2022 Annual Meeting, the House of Delegates referred Resolution 025-A-22 (Resolution 025), "Use of Social Media for Product Promotion and Compensation" which asked that the American Medical Association (AMA) "study the ethical issues of medical students, residents, fellows, and physicians endorsing non-health related products through social and mainstream media for personal or financial gain."

This report by the Council on Ethical and Judicial Affairs (CEJA) explores ethical issues posed by this use of social media and reviews existing guidance in the AMA *Code of Medical Ethics* (*Code*).

BACKGROUND

Resolution 025 details the recent phenomenon of physicians' involvement in promotions and endorsements on social media. While Resolution 025 is limited to the context of physicians promoting non-health related products through social media, it also raises issues connected to the practice of physicians selling and promoting products and services in general. As such, this report discusses a range of issues associated with the sale and promotion of all types of products, as well as the use of social media specifically for this purpose. "Sale" refers to a physician's actual selling of a product or service to consumers for financial or other consideration. Products or services may be sold from a physician's office, via the internet, or from a business venture separate from the physician's practice of medicine. "Promotion" refers to a physician's advertising of a product or service that they are personally selling or the compensated endorsement of another entity's product or services. Products or goods may be promoted via traditional media or via the internet or social media.

The ethical concerns of physician sales and promotions of both health-related and non-health related products and services are interrelated and worth exploring holistically, rather than separately as Resolution 025 suggests.

Additionally, the concept of social media has changed dramatically in the last couple of decades and has altered how consumer goods and services are advertised, promoted, and sold. Social media now accounts for a broad range of communication—e.g. Tik Tok, Instagram, Facebook, X (formerly Twitter), YouTube—that can reach millions of people, and now often involves "influencing", where individuals promote or sell goods and services or promote themselves (e.g. their personality or lifestyle) as a financial venture.

ETHICAL CONCERNS

Physicians' and medical students' sale and promotion of products or services and use of social media raises several ethical concerns. (1) These practices may damage the patient-physician relationship. If patients feel pressured to purchase products or services, this may undermine the trust that grounds patient-physician relationships, since it raises questions about whether physicians are fulfilling their fiduciary duty to put patients' interests above their own financial interests. (2) If inappropriate pressure is applied, then selling and promotion of products may result in the exploitation of patient vulnerability. (3) If physicians lend their credibility as medical professionals to products or services that are not supported by peer-reviewed evidence or are of questionable value, then they may put patient well-being and the integrity of the profession in jeopardy in the interest of profit-making.

Welfare of the Patient and the Patient-Physician Relationship

The sale and promotion of goods and services by physicians has the potential to negatively affect the welfare of patients. If a physician puts their financial interests above the interests of the patients, then this undercuts the foundational ethical principle that physicians must regard their "responsibility to the patient as paramount. [Principle VIII]. In addition, since patients are "vulnerable and dependent on the doctor's expertise" and there is an

"asymmetry of knowledge" between patients and physicians, there is a risk that patients may be exploited and this, in turn, can "undermine a patient's trust" [1]. Further, if patients find out about a physician's financial incentive to recommend certain products or services after the fact, they may feel that they have been purposefully deceived, and so have reason to distrust both that individual physician and the profession as a whole. It is therefore imperative that physicians conscientiously distinguish when they are acting in their professional capacity by recommending products or services intended for patient benefit or public health, and when they are acting as commercial agents independent of their professional identity.

Integrity of the Profession

Physician sales and promotion of products and services may also damage the integrity of the profession. Physicians have an ethical duty to uphold professional standards in their role as physician in all areas of life. A key principle of professional integrity is that physicians should recognize that they carry the authority of their professional role with them into other social spheres. Physicians "engage in a number or roles" which include conveyors of information, advocates, experts, and commentators on medically related issues [2]. For many physicians, "navigating successfully among the potentially overlapping roles …poses challenges."[2] Physicians "carry with them heightened expectations as trusted…representatives of the medical profession." [2] Physicians should be aware that these expectations cannot be entirely separated from their personal identity either online or elsewhere and should take care to curate their social media presence accordingly.

PHYSICIAN SALES AND PROMOTIONS

The *Code* addresses the ethical concerns reflected above--both with regards to the physician sale of health and non-health related products--in Opinion 9.6.4, "Sale of Health Related Products" and Opinion 9.6.5,"Sale of Non-Health Related Goods". Opinion 9.6.4 directly acknowledges conflict of interest and states that "[p]hysician sale of health-related products raises ethical concerns about financial conflict of interest, risks placing undue pressure on the patient, threatens to erode patient trust, undermine the primary obligation of physicians to serve the interests of their patients before their own, and demean the profession of medicine." It specifies that physicians have obligations to offer only peer-reviewed products, to "fully disclos[e] the nature of their financial interest," to limit "sales to products that serve immediate and pressing needs to their patients," and to avoid exclusive distributorships. Opinion 9.6.5 acknowledges the importance of physicians serving "the interests of their patients above their own" and explains that sales of non-health related goods can be acceptable under the following conditions: when the goods being sold are "low cost," when a physician takes "no share in profit" from such sales, or when the sales are "for the benefit of community organizations."

While the guidance offered by these opinions is valuable and relevant, it is limited to only some of the possible contexts in which physicians are promoting products and services, and does not include the social media scenario outlined in Resolution 025. These opinions also do not reflect the reality of physicians being involved with side businesses that are independent of their medical practices. Opinion 9.6.5 seems to suggest that physicians selling non-health-related products are doing so only for the good of the patient and should not expect to make a profit on these ventures, which is unrealistic.

Health-related products or services marketed to patients

This scenario is the one most closely aligned and envisioned by the guidance offered in Opinion 9.6.4, which encompasses the context of a physician selling health-related products (often in their office), marketed directly to their patients. Patients are often "vulnerable and dependent" on the physician's expertise" [3], so when a health-related product is promoted to a patient (especially in the physician's office) the power imbalance in the relationship makes the ethical risk particularly acute. Additionally, because the products in question are health-related, it also carries physician obligations to ensure that the products are peer reviewed and safe and that proper disclosure of the risks and benefits are given to patients. [Opinion 9.6.4]. To avoid taking advantage of patients, sale of health-related goods should be limited to only to those that serve their immediate needs, and goods should be offered at a reasonable cost.

Health-related products or services marketed to the general public

An example of this scenario might be where a physician has some side business or paid promotion to sell a health-related good, but the business is aimed at the general public. It is not performed in a physician's office nor specifically directed at patients. Hence, in most cases like this, the concern about harming the patient-physician relationship is somewhat minimized. However, it is still the case that the well-being of the general public should not be diminished for the financial gain of the physician. In all cases of the sale and promotion of health-related goods, physicians must disclose the nature of their financial interest in the product or service, and ensure that they only promote products offering benefits supported by peer-reviewed scientific evidence.

Non-health related product or service marketed to patients

This scenario is the one envisioned by the guidance of Opinion 9.6.5, which encompasses physicians selling non-health related products to their patients. An example in this case might be where a physician has a side business unrelated to their practice, but they promote the business in their office and to their patients. Here, there still may be improper influence upon the patient and such behavior may impact the trust of the patient-physician relationship while also undermining professional integrity. Opinion 9.6.5. reflects these concerns by requiring that physicians conduct such sales in a "dignified manner" and that "patients are not pressured in to making purchases" [Opinion 9.6.5]. In general, physicians should refrain from leveraging their professional role as physicians to promote unrelated business ventures and should not allow the sale or promotion of non-health-related goods or services to be a regular part of their practice of medicine.

Non-health related products to marketed to the general public

This scenario involves physicians who are selling or promoting non-health related products or services and marketing them to the general public. An example is when a physician operates a side business, such as a restaurant or a used-car dealership, and the business is promoted through the usual channels to a wide audience. This is the scenario imagined in Resolution 025, where physicians are promoting non-health-related goods through social media. Physicians should be mindful that it is still possible that patients could be customers of a physician's "side business," and in such contexts, patients may still feel pressured to become customers. Additionally, physicians must take care not to abuse their professional authority in such commercial activities and thus risk demeaning the profession. Such abuses of authority might include wearing a white coat or emphasizing medical professional credentials while selling or promoting a product. Physicians should also ensure that the information they provide about non-health-related products is trustworthy and not deceptive.

PROFESSIONALISM IN THE USE OF SOCIAL MEDIA

The concept of social media has changed since the technology's first appearance and widespread adoption. Today, social media are broadly internet-enabled technologies that enable individuals to have a presence online and ability to share opinions and self-generated media content to a wide audience.

Opinion 2.3.2 "Professionalism in Social Media" reflects an outdated understanding of the types and uses of social media, modeling its guidance on traditional sites such as Facebook, where the primary purposes are social networking among friends and colleagues, and perhaps also disseminating beneficial public health messages. While guidance that addresses these uses is still necessary (and so should be retained), modifications are required to reflect the fact that social media can now be used as a form of marketing intended to financially benefit individuals and corporations. The ethical concerns that arise in this context mirror those that arise in other situations where physicians are selling and promoting goods and services, that is, use of social media by medical professionals can undermine trust and damage the integrity of patient-physician relationships and the profession as a whole when physicians inappropriately use their social media presence to promote personal interests.

CONCLUSION

Combining the relevant parts of Opinion 9.6.4 and Opinion 9.6.5 into a single opinion and broadening the scope will allow for the *Code* to better address the full range of scenarios in which physicians may now sell and promote products or services. Updating 2.3.2 "Professionalism in the Use of Social Media" so that it includes guidance on using thes media to sell and promote products makes it clear that the consolidated guidance clearly applies to the concerns raised in Resolution 025. Revising these opinions also provides an opportunity to update language to reflect the current realities of technology and contemporary business practices.

RECOMMENDATION

In consideration of the foregoing, the Council on Ethical and Judicial Affairs recommends that:

1. Opinion 9.6.4, "Sale of Health-Related Products," and Opinion 9.6.5, "Sale of Non-Health-Related Products" be consolidated and amended by substitution to read as follows:

   The sale or promotion of products or services by physicians may offer benefit to patients or the public but may also conflict with their professional ethical responsibilities. Whether intended or not, they may be perceived to use their professional knowledge and stature as inducements to consumers. There are four key scenarios of sales or promotion: (1) health-related products or services marketed to patients, (2) health-related products or services marketed to the general public, (3) non-health-related product or services marketed to patients, and (4) non-health-related products or services marketed to the general public.

   Of greatest concern are commercial practices in which physicians sell or promote goods or services to patients. In these circumstances patients may feel pressured to purchase the product or service, which may compromise the physician's fiduciary obligation to put patients' interests above their own financial interests and undermine the trust that grounds patient-physician relationships. Similarly, if physicians lend their credibility as medical professionals to products or services that are not supported by peer-reviewed evidence or are of questionable value they may put patient well-being and the integrity of the profession in jeopardy.

   Physicians and medical students therefore should:

   (a) Refrain from leveraging their professional role to promote unrelated business ventures.

   (b) Fully disclose the nature of their financial interest in the product or service.

   (c) Avoid exclusive distributorship arrangements that make products or services available only through the individual's commercial venue.

   (d) Limit the sale or promotion of health-related goods or services only to those that serve the immediate needs of patients and strive to make the product or service available at a reasonable cost.

   (e) Refrain from the sale or promotion of non-health-related goods or services as a regular part of their professional activities; and

2. Opinion 2.3.2, "Professionalism in the Use of Social Media" be amended by substitution to read as follows:

   Social media—internet-enabled communication technologies—enable individual medical students and physicians to have both a personal and a professional presence online. Social media can foster collegiality and camaraderie within the profession as well as provide opportunities to disseminate public health messages and other health communication widely. However, use of social media by medical professionals can also undermine trust and damage the integrity of patient-physician relationships and the profession as a whole, especially when medical students and physicians use their social media presence to promote personal interests.

   Physicians and medical students should be aware that they cannot realistically separate their personal and professional personas entirely online and should curate their social media presence accordingly. Physicians and medical students therefore should:

   (a) Use caution when publishing any content that could damage their individual professional reputation or impugn the integrity of the profession.

   (b) Respect professional standards of patient privacy and confidentiality and refrain from publishing identifiable patient information online. When they use social media for educational purposes or to exchange information professionally with other physicians or medical students they should follow ethics guidance regarding confidentiality, privacy, and informed consent.

(c) Maintain appropriate boundaries of the patient-physician relationship in accordance with ethics guidance if they interact with patients through social media, just as they would in any other context.

(d) Use privacy settings to safeguard personal information and content, but be aware that once on the Internet, content is likely there permanently. They should routinely monitor their social media presence to ensure that their personal and professional information and content published about them by others is accurate and appropriate.

(e) Disclose any financial interests related to their social media content, including, but not limited to, paid partnerships and corporate sponsorships.

(f) When using social media platforms to disseminate medical health care information, ensure that such information is useful and accurate. They should likewise ensure to the best of their ability that non-health-related information is not deceptive. (Modify HOD/CEJA Policy); and

3. The remainder of this report be filed.

2. RESEARCH HANDLING OF DE-IDENTIFIED PATIENT DATA

Reference committee hearing: see report of Reference Committee on Amendments to Constitution and Bylaws.

HOUSE ACTION: REFERRED

Policy D-315.969, "Research Handling of De-Identified Patient Data," adopted by the American Medical Association (AMA) House of Delegates in November 2021, asked the Council on Ethical and Judicial Affairs (CEJA) to examine guidance related to the use of de-identified patient data and the risks of re-identification.

In its informational report on de-identified data [CEJA 6-A-23], CEJA examined a range of challenges that health care professionals and institutions are now confronted with as technological innovations rapidly evolve both within and outside of health care, blurring the boundary distinctions between these spheres. The Council's exploration suggested that in this dynamic environment, foundational ethical concepts of privacy and consent likely need to be revisited to better reflect that personal health information today exists in digital environments where responsibilities are distributed among multiple stakeholders.

This report expands on the previous work to articulate a series of recommendations on how best to respond to the increasing collection, sale, and use of de-identified patient data and the associated risks. The report outlines how health data exist within digital information ecosystems, how such ecosystems pose challenges to data privacy, what the *Code* says about data privacy and informed consent, how de-identified data functions as a public good for clinical research, how privacy scholars are reconceptualizing privacy as contextual integrity, and how de-identified data derived within the context of health care institutions lead to certain ethical standards for and protections of that data.

Because CEJA recognizes both the promise of de-identified datasets for advancing health and the concerns surrounding the use of de-identified patient data including the risks of re-identification that extend from the level of individual physicians collecting clinical data to hospitals and other health care institutions as repositories and stewards of data, this report proposes a new ethics opinion in conjunction with amendments to four existing opinions to provide ethics guidance in this rapidly evolving digital health ecosystem.

HEALTH DATA & DIGITAL ECOSYSTEMS

De-identified patient data are a subset of health data that exists within larger digital health information ecosystems [1]. Such ecosystems are highly dynamic and distributed, with health information often being combined from multiple datasets and distributed among multiple stakeholders [1]. Traditionally, health data has referred to patient health information produced from patient–physician interactions and stored by health care organizations [2]. This

type of data is typically recorded as identifiable patient data and entered into the patient's Electronic Medical Record (EMR); from there, it can be de-identified and bundled together with other patent data to form an aggregated dataset. In the age of Big Data, however, where large datasets can reveal complex patterns and trends, diverse sets of information are increasingly brought together. Health data now extends to all health-relevant data, including data collected anywhere from individuals both passively and actively that can reveal information about health and health care use [2].

Within digital health ecosystems, health-related data can be generated by health care systems (e.g., EMRs, prescriptions, laboratory data, radiology), the consumer health and wellness industry (e.g., wearable fitness tracking devices, wearable medical devices such as insulin pumps, home DNA tests), digital exhaust from daily digital activities (e.g., social media posts, internet search histories, location and proximity data), as well as non-health sources of data (e.g., non-medical records of race, gender, education level, residential zip code, credit history) [2]. The ethical challenges raised by such widely distributed data ecosystems, with their vast array of data types and multiple stakeholders, require a holistic approach to the moral issues caused by digital innovation. Digital ethics has arisen as a theoretical framework to analyze these recent challenges and examine such ethical concerns from multiple levels of abstraction. The digital ethics framework takes into account the general environment in which ethical concerns arise and examines ethical dilemmas as they relate to information and data, algorithms, practices and infrastructure, and their impact on the digital world [3].

CHALLENGES TO DATA PRIVACY

In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) imposes constraints on the sharing of "protected health information," including individually identifiable health information contained in the EMR, by "covered entities," including physicians, hospitals, pharmacies, and third-party payers. HIPAA's scope is narrow and does not cover other health-relevant data, such as data generated voluntarily by patients themselves, for example, through the use of commercial health-related apps or devices, or identifiable data individuals provide to municipal authorities, utilities, retailers, or on social media. Furthermore, information that began in the medical record can take on a new, independent life when linked with personal information widely available through datasets generated outside of health care. As McGraw and Mandl explain, "since HIPAA's coverage is about 'who' holds the data, but not what type of data, much of the health-relevant data collected today are collected by entities outside of HIPAA's coverage bubble and thus resides outside of HIPAA's protections" [2]. HIPAA is thus limited in its ability to protect patient data within digital health information ecosystems.

Complicating the matter is the fact that once patient health data has been de-identified, it is no longer protected by HIPAA, and can be freely bought, sold, and combined with other datasets. Hospitals now frequently sell de-identified datasets to researchers and industry. Recent developments in AI and its use within health care have similarly created new difficulties. While many within health care are hopeful that the use of generative AI technologies will improve care and efficiency, the input of any identifiable private health information into an AI chatbot from a private company that has not signed an agreement with the health care institution means the input of any private health information is an unauthorized disclosure under HIPAA [4].

Patients, and patient privacy advocates, are often concerned about who has access to their data. As data ecosystems have grown larger and more distributed, this has become increasingly more difficult to ascertain. In the age of Big Data, the global sale of data has become a multibillion-dollar industry, with individuals' data viewed by industry as "new oil" [1]. Industry often purchases hospital datasets to improve marketing and sales, predict consumer behaviors, and to resell to other entities. Within health care and research settings, the massive datasets collected from clinical data—used initially in the care and treatment of individual patients—have created the potential for secondary use as a means for quality improvement and innovation that can be used for the benefit of future patients and patient populations [5].

The dynamic and distributed nature of today's digital health information ecosystems challenges the prevailing procedural model for protecting patient privacy: informed consent and de-identification. In a world where the secondary use of patient data within large datasets can easily enter into a global marketplace, the intended use is

almost impossible to discern. Patients cannot be honestly and accurately informed about the specific terms of interactions between their collected data and the data collector and any potential risks that may emerge [1,6]. Therefore, patients are unable to truly give informed consent. Furthermore, whether de-identifying datasets truly prevents individual data subjects from being re-identified has been increasingly called into question. Removing the 18 identifiers specified in HIPAA does not ensure that the data subject cannot be re-identified by triangulation with identifying information from other readily available datasets [7]. Machine learning and AI technologies have advanced to the point that virtually all de-identified datasets risk re-identification, such that "even when individuals are not 'identifiable', they may still be 'reachable'" [6].

A final avenue to consider with respect to private health information and patient privacy is the risk of health care data breaches. Raghupathi et al note, "[h]ealthcare is a lucrative target for hackers. As a result, the healthcare industry is suffering from massive data breaches" [8]. The number of health care data breaches continues to increase every year, exposing the private health information of millions of Americans. Despite being heavily targeted by cybercriminals, health care providing institutions are widely considered by cybersecurity experts to lack sufficient security safeguards [8]. Raghupathi et al note, "healthcare entities gathering and storing individual health data have a fiduciary and regulatory duty to protect such data and, therefore, need to be proactive in understanding the nature and dimensions of health data breaches" [8].

CLINICAL DATA AND PRIVACY

Within the *Code,* Opinion 3.1.1, "Privacy in Health Care," distinguishes four aspects of privacy:

> personal space (physical privacy), personal data (informational privacy), personal choices including cultural and religious affiliations (decisional privacy), and personal relationships with family members and other intimates (associational privacy).

The *Code* does not explicitly examine whether personal medical or health information are ethically distinct from other kinds of personal information (e.g., financial records) or in what way. Current guidance treats the importance of protecting privacy in all its forms as self-evident, holding that respecting privacy in all its aspects is of fundamental importance, "an expression of respect for autonomy and a prerequisite for trust" [Opinion 3.1.1]. However, Opinion 3.3.3, "Breach of Security in Electronic Medical Records," directly acknowledges that data security breaches create potential "physical, emotional, and dignity harms" to patients. Similarly, Opinion 7.3.7, "Safeguards in the Use of DNA Databanks," states that breaches of confidential patient information "may result in discrimination or stigmatization and may carry implications for important personal choices."

Violations of privacy can result in both harm—tangible negative consequences, such as discrimination in insurance or employment or identity theft—and in wrongs that occur from the fact of personal information being known without the subject's awareness, even if the subject suffers no tangible harm [7]. Price and Cohen note that privacy issues can arise not only when data are known, but when data mining enables others to "generate knowledge about individuals through the process of inference rather than direct observation or access" [7].

CLINICAL DATA AND INFORMED CONSENT

With respect to Opinion 2.1.1, "Informed Consent," in the *Code,* successful communication is seen as essential to fostering trust that is fundamental to the patient–physician relationship and to supporting shared decision making. Opinion 2.1.1 states: "[t]he process of informed consent occurs when communication between a patient and physician results in the patient's authorization or agreement to undergo a specific medical intervention." In seeking a patient's informed consent, physicians are directed to include information about "the burdens, risks, and expected benefits of all options, including forgoing treatment" [Opinion 2.1.1]. It should be noted, however, that no direct mention of patient data is discussed in the opinion, other than that documentation of consent should be recorded in the patient's medical record.

CLINICAL DATA, DATASETS, AND THE PUBLIC GOOD

While legally, clinical data are the property of the health care organization, ethically, because such aggregated data has the potential for secondary use that can benefit all of society, it has been argued that such data should be treated as a form of public good [5]. When clinical data are de-identified and aggregated, the potential use for societal benefits through research and development is an emergent, secondary side effect of electronic health records that goes beyond individual benefit. Larson et al argue that not only does the public possess an interest in safeguarding and promoting clinical data for societal benefits, but all those who participate in health care systems have an ethical responsibility to treat such data as a form of public good [5]. They propose:

> all individuals and entities with access to clinical data inherently take on the same fiduciary obligations as those of medical professionals, including for-profit entities. For example, those who are granted access to the data must accept responsibility for safeguarding protected health information [5].

This entails that any entity that purchases private health information, whether or not it has been de-identified, has an ethical obligation to adhere to the ethical standards of health care where such data were produced. Hospitals thus have an ethical responsibility to ensure that their contracts of sale for datasets insist that all entities that gain access to the data adhere to the ethical standards and values of the health care industry.

This is particularly important when we recall that the wide distribution of digital health information ecosystems increasingly includes non-health-related parties from industry that may have market interests that conflict with the ethical obligations that follow health data. Within this framework, the fiduciary duty to protect patient privacy as well as to society to improve future health care follows the data and thus applies to all entities that use that data, such that all entities granted access to the data become data stewards, including for-profit parties [5]. This also includes patients, such that they bear a responsibility to allow their data to be used for the future improvement of health care for society, especially when we recognize that current health care has already benefited from past data collection [5].

While the re-identification of aggregated patient data should generally be prohibited, there are rare exceptions. There may be occasions when researchers wish to re-identify a dataset, such as sometimes occurs in the study of rare diseases that rely on international registries; in such situations, all individuals must be re-contacted, and their consent obtained in order to re-identify their data since this would represent a significant change to the initial research protocols and respective risks [9]. Re-identification of datasets for research is uncommon, however, because obtaining re-consent can be difficult and can lead to flawed research if data is lost because patients do not re-consent. The other situation in which it may be permissible, or even obligatory, to re-identify aggregated patient data is when doing so would be in the interest of the health of individual patients, such as might occur in the study of a rare genetic disorder. Even within these exceptions, the risks associated with re-identification remain and re-identified data should thus never be published. Re-identification of de-identified patient data for any other purposes, by anyone inside or outside of health care, must be avoided.

AN ALTERNATIVE APPROACH: PRIVACY AS CONTEXTUAL INTEGRITY

Within today's digital health information ecosystems, physicians and hospitals face several challenges to protecting patient privacy. Barocas and Nissenbaum contend that "even if [prevailing forms of consent and anonymization] were achievable, they would be ineffective against the novel threats to privacy posed by big data" [6]. A more effective option, Nissenbaum has argued, would understand privacy protection as a function of "contextual integrity," i.e., that in a given social domain, information flows conform to the context-specific informational norms of that domain. Whether a transmission of information is appropriate depends on "the type of information in question, about whom it is, by whom and to whom it is transmitted, and conditions or constraints under which this transmission takes place" [10]. The view of privacy as contextual integrity—that our conception of privacy is contextual and governed by various norms of information flow—recognizes that there exist different norms regarding privacy within different spheres of any distributed digital ecosystem [7,11]. The challenge within health care, as we have seen, is how to balance these various norms when they conflict and how to ensure that health care's

ethical standards and values are maintained throughout the distributed use of de-identified private health information.

THE CONTEXTUAL INTEGRITY OF DE-IDENTIFIED HEALTH DATA

In handling patient data, individual physicians strive to balance supporting and respecting patient privacy while also upholding ethical obligations to the betterment of public health. Through their own actions, as well as through their membership organizations and through their healthcare organizations, physicians should: (1) ensure that data entered into electronic records are accurate and reliable to the best of their ability; (2) be transparent with patients regarding the limited extent to which their data can be safely protected, how their data may be used, and why the use of such data is crucial for improving health care outcomes within society; and (3) ensure that proper oversight and protections of data are in place, including contractual provisions that any data sold or shared with outside entities stay in alignment with the ethical standards of the medical profession, and that meaningful sanctions or penalties are in place and enforced against any actors that violate those ethical standards. It is critical to recognize, as is outlined in the *Code,* that the patient–physician relationship is built on trust, and that this trust relies heavily on transparency.

It is important for both patient care and research that clinical data entered into the EMR be as accurate and complete as possible. Some data capture practices, such as copying-and-pasting daily progress notes from previous encounters, which may contribute to efficiency, can lead to documentation errors [12]. One avenue for improving EMR accuracy is that, under HIPAA, patients have the right to access their data and request any perceived errors be amended. While there is no one solution to improving accuracy of EMR data, further study into how to improve EMR accuracy is important. One challenge to both EMR accuracy and completeness is the limited interoperability of different EMR systems. Matching digital health records for the same patient across and within health care facilities can be a challenge, further contributing to the potential for EMR errors. Standardization of recording data elements, such as capturing patient address and last name in a consistent format, may improve matching of patient records and thus improve the accuracy of the EMR [13].

Another challenge to EMR data quality is the risk of bias, primarily due to implicit bias in EMR design and underrepresentation of patients from historically marginalized groups, low socioeconomic status, and rural areas [14,15]. Critically important for research involving data collected from EMRs, available EMR data only reflects those with access to health care in the first place. While certain study designs and tools have been developed to reduce these biases in research, physicians and health care institutions should be looking into ways to reduce bias within EMRs, such as features to optimize effective EMR use and to consistently capture patient data, especially data on race/ethnicity and social determinants of health that are often inconsistently and inaccurately captured in EMR systems [14,15,16].

Patients have a right to know how and why their data are being used. While physicians should be able to answer questions regarding patient data as they relate to HIPAA protections, it is the responsibility of health care institutions to provide more detailed information regarding expectations of data privacy, how patient data may be used, and why such use is important to improve the future of health care. Health care systems may consider fulfilling this ethical obligation by creating a patient notification of data use built into the patient registration process (using language similar to the NIH's Introduction-Description component, meant to provide prospective research participants with an introduction to and description of the planned storage and sharing of data and biospecimens [17]).
As stewards of health data, health care institutions have an ethical responsibility to protect data privacy. This fiduciary duty to patient data should be seen as following the data even after they are de-identified and leave the institution where they were initially captured [5,8]. While hospitals and health care organizations increasingly come under cyberattack, they consistently lag behind other industries in cybersecurity [18]. With regards to protecting the data they maintain, health care institutions have a responsibility to make more significant investments in cybersecurity.

In order to ensure that the ethical standards of health care are maintained even after data leaves health care institutions, McGraw and Mandl propose that companies collecting or using health-relevant data could be required to establish independent data ethics review boards [2]. They write that such boards could be similar to Institutional

Review Boards (IRBs) but should focus more on privacy than on participant risk, evaluating proposed data projects for legal and ethical implications as well as their potential to improve health and/or the health care system [2]. In practice, ethics review boards involved with industry face challenges to both independence and efficacy. Independence can be compromised by influences such as conflicts of interest, while efficacy can be compromised by the absence of authority, procedures, and systems to enact recommendations made by these review bodies. To be effective, data ethics review boards must be independent and free of conflicts of interest from the company or organization whose data research proposal(s) they are evaluating and have systems in place for both transparency and implementation of feedback for remediations of privacy and other quality and ethics concerns. Though not a comprehensive solution, independent data ethics review boards could be an effective safeguard against industry conflicts of interest and should be considered as a required part of contracts of sale of health data, with contracts stipulating that any future resale of the data also undergo review by a data ethics review board.

The need for more transparent disclosure to patients regarding their data use as well as the importance of building the values of medical ethics into the contracts of sale of aggregate datasets created by hospitals highlights the fact that the ethical responsibilities to respond to the risks of de-identified data should not be borne by physicians alone. Respecting patient privacy and their informed consent are responsibilities that physician member organizations and health care institutions must take on because the risks to these rights that patients face within digital health ecosystems radiate far beyond the patient–physician relationship to areas where individual physicians have little influence.

RECOMMENDATIONS

In light of the challenges considered with regard to constructing a framework for holding stakeholders accountable within digital health information ecosystems, the Council on Ethical and Judicial Affairs recommends:

1. That the following be adopted:

    Within health care systems, identifiable private health information, initially derived from and used in the care and treatment of individual patients, has led to the creation of massive de-identified datasets. As aggregate datasets, clinical data takes on a secondary promising use as a means for quality improvement and innovation that can be used for the benefit of future patients and patient populations. While de-identification of data is meant to protect the privacy of patients, there remains a risk of re-identification, so while patient anonymity can be safeguarded it cannot be guaranteed. In handling patient data, individual physicians thus strive to balance supporting and respecting patient privacy while also upholding ethical obligations to the betterment of public health.

    When clinical data are de-identified and aggregated, their potential use for societal benefits through research and development is an emergent, secondary use of electronic health records that goes beyond individual benefit. Such data, due to their potential to benefit public health, should thus be treated as a form of public good, and the ethical standards and values of health care should follow the data and be upheld and maintained even if the data are sold to entities outside of health care. The medical profession's responsibility to protect patient privacy as well as to society to improve future health care should be recognized as inherently tied to these datasets, such that all entities granted access to the data become data stewards with a duty to uphold the ethical values of health care in which the data were produced.

    As members of health care institutions, physicians should:

    (a) Follow existing and emerging regulatory safety measures to protect patient privacy;
    (b) Practice good data intake, including collecting patient data equitably to reduce bias in datasets;
    (c) Answer any patient questions about data use in an honest and transparent manner to the best of their ability in accordance with HIPAA (or current legal standards).

Health care systems, in interacting with patients, should adopt policies and practices that provide patients with transparent information regarding:

(d) The high value that health care institutions place on protecting patient data;
(e) The reality that no data can be guaranteed to be permanently anonymized, and that risk of re-identification does exist;
(f) How patient data may be used and by whom;
(g) The importance of de-identified aggregated data for improving the care of future patients.

Health care systems, as health data stewards, should:

(h) Establish appropriate data collection methods and practices that meet industry standards to ensure the creation of high-quality datasets;
(i) Ensure proper oversight of patient data is in place, including provisions for the use of de-identified datasets that may be shared, sold, or resold;
(j) Develop models for the ethical use of de-identified datasets when such provisions do not exist, such as establishing and contractually requiring independent data ethics review boards free of conflicts of interest to evaluate the sale and potential resale of clinically-derived datasets;
(k) Take appropriate cyber security measures to ensure the highest level of protection is provided to patients and patient data;
(l) Develop proactive post-compromise planning strategies for use in the event of a data breach to minimize additional harm to patients;
(m) Advocate that health- and non-health entities using any health data adopt the strongest protections and uphold the ethical values of the medical profession.

There is an inherent tension between the potential benefits and burdens of de-identified datasets as both sources for quality improvement to care as well as risks to patient privacy. Re-identification of data may be permissible, or even obligatory, in rare circumstances when done in the interest of the health of individual patients. Re-identification of aggregated patient data for other purposes without obtaining patients' express consent, by anyone outside or inside of health care, is impermissible; and

2. That Opinion 2.1.1, "Informed Consent"; Opinion 3.1.1, "Privacy in Health Care"; Opinion 3.2.4, "Access to Medical Records by Data Collection Companies"; and Opinion 3.3.2, "Confidentiality and Electronic Medical Records" be amended by addition as follows:

a. Opinion 2.1.1, Informed Consent

Informed consent to medical treatment is fundamental in both ethics and law. Patients have the right to receive information and ask questions about recommended treatments so that they can make well-considered decisions about care. Successful communication in the patient-physician relationship fosters trust and supports shared decision making. Transparency with patients regarding all options of treatment is critical to establishing trust and should extend to discussions regarding who has access to patients' health data and how data may be used.

The process of informed consent occurs when communication between a patient and physician results in the patient's authorization or agreement to undergo a specific medical intervention. In seeking a patient's informed consent (or the consent of the patient's surrogate if the patient lacks decision-making capacity or declines to participate in making decisions), physicians should:

(a) Assess the patient's ability to understand relevant medical information and the implications of treatment alternatives and to make an independent, voluntary decision.
(b) Present relevant information accurately and sensitively, in keeping with the patient's preferences for receiving medical information. The physician should include information about:
(i) the diagnosis (when known);
(ii) the nature and purpose of recommended interventions;
(iii) the burdens, risks, and expected benefits of all options, including forgoing treatment.

(c) Document the informed consent conversation and the patient's (or surrogate's) decision in the medical record in some manner. When the patient/surrogate has provided specific written consent, the consent form should be included in the record.

In emergencies, when a decision must be made urgently, the patient is not able to participate in decision making, and the patient's surrogate is not available, physicians may initiate treatment without prior informed consent. In such situations, the physician should inform the patient/surrogate at the earliest opportunity and obtain consent for ongoing treatment in keeping with these guidelines.

b. Opinion 3.1.1, Privacy in Health Care

Protecting information gathered in association with the care of the patient is a core value in health care. However, respecting patient privacy in other forms is also fundamental, as an expression of respect for patient autonomy and a prerequisite for trust.

Patient privacy encompasses a number of aspects, including personal space (physical privacy), personal data (informational privacy), personal choices including cultural and religious affiliations (decisional privacy), and personal relationships with family members and other intimates (associational privacy).

Physicians must seek to protect patient privacy in all settings to the greatest extent possible and should:

(a) Minimize intrusion on privacy when the patient's privacy must be balanced against other factors.
(b) Inform the patient when there has been a significant infringement on privacy of which the patient would otherwise not be aware.
(c) Be mindful that individual patients may have special concerns about privacy in any or all of these areas.
(d) Be transparent that privacy safeguards for patient data are in place but acknowledge that anonymity cannot be guaranteed and that breaches can occur notwithstanding best data safety practices.

c. Opinion 3.2.4, Access to Medical Records by Data Collection Companies

Information contained in patients' medical records about physicians' prescribing practices or other treatment decisions can serve many valuable purposes, such as improving quality of care. However, ethical concerns arise when access to such information is sought for marketing purposes on behalf of commercial entities that have financial interests in physicians' treatment recommendations, such as pharmaceutical or medical device companies.

Information gathered and recorded in association with the care of a patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship.

Physicians who propose to permit third-party access to specific patient information for commercial purposes should:

(a) Only provide data that has been de-identified.
(b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity) about the purpose(s) for which access would be granted.

Physicians who propose to permit third parties to access the patient's full medical record should:

(c) Obtain the consent of the patient (or authorized surrogate) to permit access to the patient's medical record.
(d) Prohibit access to or decline to provide information from individual medical records for which consent has not been given.
(e) Decline incentives that constitute ethically inappropriate gifts, in keeping with ethics guidance.

Because de-identified datasets are derived from patient data as a secondary source of data for the public good, health care professionals and/or institutions who propose to permit third-party access to such information have a responsibility to ensure that any use of data derived from health care adhere to the ethical standards of the medical profession.

d. Opinion 3.3.2, Confidentiality and Electronic Medical Records

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.

Physicians who collect or store patient information electronically, whether on stand-alone systems in their own practice or through contracts with service providers, must:

(a) Choose a system that conforms to acceptable industry practices and standards with respect to:
  (i) restriction of data entry and access to authorized personnel;
  (ii) capacity to routinely monitor/audit access to records;
  (iii) measures to ensure data security and integrity; and
  (iv) policies and practices to address record retrieval, data sharing, third-party access and release of information, and disposition of records (when outdated or on termination of the service relationship) in keeping with ethics guidance.
(b) Describe how the confidentiality and integrity of information is protected if the patient requests.
(c) Release patient information only in keeping with ethics guidance for confidentiality and privacy; and

3. That the remainder of this report be filed.