

AMA Code of Medical Ethics

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 establish that any use of data derived from health care adhere to the ethical standards of the medical profession.

AMA Principles of Medical Ethics: I,II,IV

Background report(s):

CEJA Report 2-A-24 Research Handling of De-Identified Patient Data

CEJA Report 3-A-16 Modernized *Code of Medical Ethics*

CEJA Report 6-A-94 Disclosure of Records to Data Collection Companies

REPORT 2 OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS (A-24)
Research Handling of De-Identified Patient Data
(D-315.969)

EXECUTIVE SUMMARY

In adopting policy D-315.969, “Research Handling of De-Identified Patient Data,” the House of Delegates directed 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.

This report articulates 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 complex ecosystems pose challenges to data privacy, how de-identified data functions as a public good for clinical research, 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 Code of Medical Ethics opinion be adopted in conjunction with amendments to four existing opinions to provide ethics guidance in this rapidly evolving digital health ecosystem.

REPORT OF THE COUNCIL ON ETHICAL AND JUDICIAL AFFAIRS*

CEJA Report 2-A-24

Subject: Research Handling of De-Identified Patient Data
(D-315.969)

Presented by: David A. Fleming, MD, Chair

Referred to: Reference Committee on Amendments to Constitution and Bylaws

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

5
6 In its informational report on de-identified data [[CEJA 6-A-23](#)], CEJA examined a range of
7 challenges that health care professionals and institutions are now confronted with as technological
8 innovations rapidly evolve both within and outside of health care, blurring the boundary
9 distinctions between these spheres. CEJA’s exploration suggested that in this dynamic environment,
10 foundational ethical concepts of privacy and consent likely need to be revisited to better reflect that
11 personal health information today exists in digital environments where responsibilities are
12 distributed among multiple stakeholders.

13
14 This report expands on the previous work to articulate a series of recommendations on how best to
15 respond to the increasing collection, sale, and use of de-identified patient data and the associated
16 risks. The report outlines how health data exist within digital information ecosystems, how such
17 ecosystems pose challenges to data privacy, what the *Code* says about data privacy and informed
18 consent, how de-identified data functions as a public good for clinical research, how privacy
19 scholars are reconceptualizing privacy as contextual integrity, and how de-identified data derived
20 within the context of health care institutions lead to certain ethical standards for and protections of
21 that data.

22
23 Because CEJA recognizes both the promise of de-identified datasets for advancing health and the
24 concerns surrounding the use of de-identified patient data including the risks of re-identification
25 that extend from the level of individual physicians collecting clinical data to hospitals and other
26 health care institutions as repositories and stewards of data, this report proposes a new ethics
27 opinion in conjunction with amendments to four existing opinions to provide ethics guidance in
28 this rapidly evolving digital health ecosystem.

* Reports of the Council on Ethical and Judicial Affairs are assigned to the Reference Committee on Amendments to Constitution and Bylaws. They may be adopted, not adopted, or referred. A report may not be amended, except to clarify the meaning of the report and only with the concurrence of the Council.

1 HEALTH DATA & DIGITAL ECOSYSTEMS

2
3 De-identified patient data are a subset of health data that exists within larger digital health
4 information ecosystems [1]. Such ecosystems are highly dynamic and distributed, with health
5 information often being combined from multiple datasets and distributed among multiple
6 stakeholders [1]. Traditionally, health data has referred to patient health information produced from
7 patient–physician interactions and stored by health care organizations [2]. This type of data is
8 typically recorded as identifiable patient data and entered into the patient’s electronic medical
9 record (EMR); from there, it can be de-identified and bundled together with other patient data to
10 form an aggregated dataset. In the age of Big Data, however, where large datasets can reveal
11 complex patterns and trends, diverse sets of information are increasingly brought together. Health
12 data now extends to all health-relevant data, including data collected anywhere from individuals
13 both passively and actively that can reveal information about health and health care use [2].
14

15 Within digital health ecosystems, health-related data can be generated by health care systems (e.g.,
16 EMRs, prescriptions, laboratory data, radiology), the consumer health and wellness industry (e.g.,
17 wearable fitness tracking devices, wearable medical devices such as insulin pumps, home DNA
18 tests), digital exhaust from daily digital activities (e.g., social media posts, internet search histories,
19 location and proximity data), as well as non-health sources of data (e.g., non-medical records of
20 race, gender, education level, residential zip code, credit history) [2]. The ethical challenges raised
21 by such widely distributed data ecosystems, with their vast array of data types and multiple
22 stakeholders, require a holistic approach to the moral issues caused by digital innovation. Digital
23 ethics has arisen as a theoretical framework to analyze these recent challenges and examine such
24 ethical concerns from multiple levels of abstraction. The digital ethics framework takes into
25 account the general environment in which ethical concerns arise and examines ethical dilemmas as
26 they relate to information and data, algorithms, practices and infrastructure, and their impact on the
27 digital world [3].
28

29 CHALLENGES TO DATA PRIVACY

30
31 In the U.S., the Health Insurance Portability and Accountability Act (HIPAA) imposes constraints
32 on the sharing of “protected health information,” including individually identifiable health
33 information contained in the EMR, by “covered entities,” including physicians, hospitals,
34 pharmacies, and third-party payers. HIPAA’s scope is narrow and does not cover other health-
35 relevant data, such as data generated voluntarily by patients themselves, for example, through the
36 use of commercial health-related apps or devices, or identifiable data individuals provide to
37 municipal authorities, utilities, retailers, or on social media. Furthermore, information that began in
38 the medical record can take on a new, independent life when linked with personal information
39 widely available through datasets generated outside of health care. As McGraw and Mandl explain,
40 “since HIPAA’s coverage is about ‘who’ holds the data, but not what type of data, much of the
41 health-relevant data collected today are collected by entities outside of HIPAA’s coverage bubble
42 and thus resides outside of HIPAA’s protections” [2]. HIPAA is thus limited in its ability to protect
43 patient data within digital health information ecosystems.
44

45 Complicating the matter is the fact that once patient health data has been de-identified, it is no
46 longer protected by HIPAA, and can be freely bought, sold, and combined with other datasets.
47 Hospitals now frequently sell de-identified datasets to researchers and industry. Recent
48 developments in AI and its use within health care have similarly created new difficulties.
49

50 Patients, and patient privacy advocates, are often concerned about who has access to their data. As
51 data ecosystems have grown larger and more distributed, this has become increasingly more

1 difficult to ascertain. In the age of Big Data, the global sale of data has become a multibillion-
2 dollar industry, with individuals' data viewed by industry as "new oil" [1]. The global health care
3 data monetization market alone was valued at just over \$0.4 billion in 2022 and is expected to grow
4 to \$1.3 billion by 2030 [4]. Industry often purchases hospital datasets to improve marketing and
5 sales, predict consumer behaviors, and to resell to other entities. Within health care and research
6 settings, the massive datasets collected from clinical data—used initially in the care and treatment
7 of individual patients—have created the potential for secondary use as a means for quality
8 improvement and innovation that can be used for the benefit of future patients and patient
9 populations [5].

10
11 The dynamic and distributed nature of today's digital health information ecosystems challenges the
12 prevailing procedural model for protecting patient privacy: informed consent and de-identification.
13 In a world where the secondary use of patient data within large datasets can easily enter into a
14 global marketplace, the intended use is almost impossible to discern. Patients cannot be honestly
15 and accurately informed about the specific terms of interactions between their collected data and
16 the data collector and any potential risks that may emerge [1,6]. Therefore, patients are unable to
17 truly give informed consent. Furthermore, whether de-identifying datasets truly prevents individual
18 data subjects from being re-identified has been increasingly called into question. Removing the 18
19 identifiers specified in HIPAA does not ensure that the data subject cannot be re-identified by
20 triangulation with identifying information from other readily available datasets [7]. Machine
21 learning and AI technologies have advanced to the point that virtually all de-identified datasets risk
22 re-identification, such that "even when individuals are not 'identifiable', they may still be
23 'reachable'" [6].

24
25 A final avenue to consider with respect to private health information and patient privacy is the risk
26 of health care data breaches. Raghupathi et al note, "[h]ealthcare is a lucrative target for hackers.
27 As a result, the healthcare industry is suffering from massive data breaches" [8]. The number of
28 health care data breaches continues to increase every year, exposing the private health information
29 of millions of Americans. Despite being heavily targeted by cybercriminals, health care providing
30 institutions are widely considered by cybersecurity experts to lack sufficient security safeguards
31 [8]. Raghupathi et al note, "healthcare entities gathering and storing individual health data have a
32 fiduciary and regulatory duty to protect such data and, therefore, need to be proactive in
33 understanding the nature and dimensions of health data breaches" [8].

34 35 CLINICAL DATA AND PRIVACY

36
37 Within the *Code*, [Opinion 3.1.1](#), "Privacy in Health Care," distinguishes four aspects of privacy:

38
39 personal space (physical privacy), personal data (informational privacy), personal choices
40 including cultural and religious affiliations (decisional privacy), and personal relationships with
41 family members and other intimates (associational privacy).

42
43 The *Code* does not explicitly examine whether personal medical or health information are ethically
44 distinct from other kinds of personal information (e.g., financial records) or in what way. Current
45 guidance treats the importance of protecting privacy in all its forms as self-evident, holding that
46 respecting privacy in all its aspects is of fundamental importance, "an expression of respect for
47 autonomy and a prerequisite for trust" [Opinion 3.1.1]. However, [Opinion 3.3.3](#), "Breach of
48 Security in Electronic Medical Records," directly acknowledges that data security breaches create
49 potential "physical, emotional, and dignity harms" to patients. Similarly, [Opinion 7.3.7](#),
50 "Safeguards in the Use of DNA Databanks," states that breaches of confidential patient information

1 “may result in discrimination or stigmatization and may carry implications for important personal
2 choices.”

3
4 Violations of privacy can result in both harm—tangible negative consequences, such as
5 discrimination in insurance or employment or identity theft—and in wrongs that occur from the
6 fact of personal information being known without the subject’s awareness, even if the subject
7 suffers no tangible harm [7]. Price and Cohen note that privacy issues can arise not only when data
8 are known, but when data mining enables others to “generate knowledge about individuals through
9 the process of inference rather than direct observation or access” [7].

10 11 CLINICAL DATA AND INFORMED CONSENT

12
13 With respect to [Opinion 2.1.1](#), “Informed Consent,” in the *Code*, successful communication is seen
14 as essential to fostering trust that is fundamental to the patient–physician relationship and to
15 supporting shared decision making. Opinion 2.1.1 states: “[t]he process of informed consent occurs
16 when communication between a patient and physician results in the patient’s authorization or
17 agreement to undergo a specific medical intervention.” In seeking a patient’s informed consent,
18 physicians are directed to include information about “the burdens, risks, and expected benefits of
19 all options, including forgoing treatment” [Opinion 2.1.1]. It should be noted, however, that no
20 direct mention of patient data is discussed in the opinion, other than that documentation of consent
21 should be recorded in the patient’s medical record.

22 23 CLINICAL DATA, DATASETS, AND THE PUBLIC GOOD

24
25 Because aggregated clinical data has the potential for secondary use that can benefit all of society,
26 it has been argued that such data should be treated as a form of public good [5]. When clinical data
27 are de-identified and aggregated, the potential use for societal benefits through research and
28 development is an emergent, secondary side effect of electronic health records that goes beyond
29 individual benefit. Larson et al argue that not only does the public possess an interest in
30 safeguarding and promoting clinical data for societal benefits, but all those who participate in
31 health care systems have an ethical responsibility to treat such data as a form of public good [5].
32 They propose:

33
34 all individuals and entities with access to clinical data inherently take on the same fiduciary
35 obligations as those of medical professionals, including for-profit entities. For example, those
36 who are granted access to the data must accept responsibility for safeguarding protected health
37 information [5].
38

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

44
45 This is particularly important when we recall that the wide distribution of digital health information
46 ecosystems increasingly includes non-health-related parties from industry that may have market
47 interests that conflict with the ethical obligations that follow health data. Within this framework,
48 the fiduciary duty to protect patient privacy as well as to society to improve future health care
49 follows the data and thus applies to all entities that use that data, such that all entities granted
50 access to the data become data stewards, including for-profit parties [5]. This also includes patients,
51 such that they bear a responsibility to allow their data to be used for the future improvement of

1 health care for society, especially when we recognize that current health care has already benefited
2 from past data collection [5].

3
4 While the re-identification of aggregated patient data should generally be prohibited, there are rare
5 exceptions. There may be occasions when researchers wish to re-identify a dataset, such as
6 sometimes occurs in the study of rare diseases that rely on international registries; in such
7 situations, all individuals must be re-contacted, and their consent obtained in order to re-identify
8 their data since this would represent a significant change to the initial research protocols and
9 respective risks [9]. Re-identification of datasets for research is uncommon, however, because
10 obtaining re-consent can be difficult and can lead to flawed research if data is lost because patients
11 do not re-consent. The other situation in which it may be permissible, or even obligatory, to re-
12 identify aggregated patient data is when doing so would be in the interest of the health of individual
13 patients, such as might occur in the study of a rare genetic disorder. Even within these exceptions,
14 the risks associated with re-identification remain and re-identified data should thus never be
15 published. Re-identification of de-identified patient data for any other purposes, by anyone inside
16 or outside of health care, must be avoided.

17 18 AN ALTERNATIVE APPROACH: PRIVACY AS CONTEXTUAL INTEGRITY

19
20 Within today's digital health information ecosystems, physicians and hospitals face several
21 challenges to protecting patient privacy. Barocas and Nissenbaum contend that "even if [prevailing
22 forms of consent and anonymization] were achievable, they would be ineffective against the novel
23 threats to privacy posed by big data" [6]. A more effective option, Nissenbaum has argued, would
24 understand privacy protection as a function of "contextual integrity," i.e., that in a given social
25 domain, information flows conform to the context-specific informational norms of that domain.
26 Whether a transmission of information is appropriate depends on "the type of information in
27 question, about whom it is, by whom and to whom it is transmitted, and conditions or constraints
28 under which this transmission takes place" [10]. The view of privacy as contextual integrity—that
29 our conception of privacy is contextual and governed by various norms of information flow—
30 recognizes that there exist different norms regarding privacy within different spheres of any
31 distributed digital ecosystem [7,11]. The challenge within health care, as we have seen, is how to
32 balance these various norms when they conflict and how to ensure that health care's ethical
33 standards and values are maintained throughout the distributed use of de-identified private health
34 information.

35 36 THE CONTEXTUAL INTEGRITY OF DE-IDENTIFIED HEALTH DATA

37
38 In handling patient data, individual physicians strive to balance supporting and respecting patient
39 privacy while also upholding ethical obligations to the betterment of public health. Through their
40 own actions, as well as through their membership organizations and through their health care
41 organizations, physicians should: (1) ensure that data entered into electronic records are accurate
42 and reliable to the best of their ability; (2) be transparent with patients regarding the limited extent
43 to which their data can be safely protected, how their data may be used, and why the use of such
44 data is crucial for improving health care outcomes within society; and (3) ensure that proper
45 oversight and protections of data are in place, including contractual provisions that any data sold or
46 shared with outside entities stay in alignment with the ethical standards of the medical profession,
47 and that meaningful sanctions or penalties are in place and enforced against any actors that violate
48 those ethical standards. It is critical to recognize, as is outlined in the *Code*, that the patient-
49 physician relationship is built on trust, and that this trust relies heavily on transparency.

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

13
14 Another challenge to EMR data quality is the risk of bias, primarily due to implicit bias in EMR
15 design and underrepresentation of patients from historically marginalized groups, low
16 socioeconomic status, and rural areas [14,15]. Critically important for research involving data
17 collected from EMRs, available EMR data only reflects those with access to health care in the first
18 place. While certain study designs and tools have been developed to reduce these biases in
19 research, physicians and health care institutions should be looking into ways to reduce bias within
20 EMRs, such as features to optimize effective EMR use and to consistently capture patient data,
21 especially data on race/ethnicity and social determinants of health that are often inconsistently and
22 inaccurately captured in EMR systems [14,15,16].

23
24 Patients have a right to know how and why their data are being used. While physicians should be
25 able to answer questions regarding patient data as they relate to HIPAA protections, it is the
26 responsibility of health care institutions to provide more detailed information regarding
27 expectations of data privacy, how patient data may be used, and why such use is important to
28 improve the future of health care. Health care systems may consider fulfilling this ethical
29 obligation by creating a patient notification of data use built into the patient registration process
30 (using language similar to the National Institutes of Health's (NIH) Introduction-Description
31 component, meant to provide prospective research participants with an introduction to and
32 description of the planned storage and sharing of data and biospecimens [17]).

33
34 As stewards of health data, health care institutions have an ethical responsibility to protect data
35 privacy. This fiduciary duty to patient data should be seen as following the data even after they are
36 de-identified and leave the institution where they were initially captured [5,8]. While hospitals and
37 health care organizations increasingly come under cyberattack, they consistently lag behind other
38 industries in cybersecurity [18]. With regards to protecting the data they maintain, health care
39 institutions have a responsibility to make more significant investments in cybersecurity.

40
41 In order to ensure that the ethical standards of health care are maintained even after data leaves
42 health care institutions, McGraw and Mandl propose that companies collecting or using health-
43 relevant data could be required to establish independent data ethics review boards [2]. They write
44 that such boards could be similar to Institutional Review Boards but should focus more on privacy
45 than on participant risk, evaluating proposed data projects for legal and ethical implications as well
46 as their potential to improve health and/or the health care system [2]. In practice, ethics review
47 boards involved with industry face challenges to both independence and efficacy. Independence
48 can be compromised by influences such as conflicts of interest, while efficacy can be compromised
49 by the absence of authority, procedures, and systems to enact recommendations made by these
50 review bodies. To be effective, data ethics review boards must be independent and free of conflicts
51 of interest from the company or organization whose data research proposal(s) they are evaluating

1 and have systems in place for both transparency and implementation of feedback for remediations
2 of privacy and other quality and ethics concerns. Though not a comprehensive solution,
3 independent data ethics review boards could be an effective safeguard against industry conflicts of
4 interest and should be considered as a required part of contracts of sale of health data, with
5 contracts stipulating that any future resale of the data also undergo review by a data ethics review
6 board.

7
8 An additional safeguard is the implementation of regular data audits to assess the quality and use of
9 shared data [19]. These regulatory measures could be implemented as requirements outlined in
10 Data Use Agreements or Data Sharing Agreements (DSAs). Such agreements have the potential to
11 establish data governance policies and practices within health care institutions regarding “what data
12 can be shared, with whom, under what conditions, and for what purposes.” In developing DSAs,
13 hospital administrators should engage all relevant stakeholders, require a neutral entity be
14 designated as an independent custodian of shared data, limit the types and/or characteristics of
15 shared data to certain purposes, and apply additional safeguards to protect the data [20].

16
17 The need for more transparent disclosure to patients regarding their data use as well as the
18 importance of building the values of medical ethics into the contracts of sale of aggregate datasets
19 created by hospitals highlights the fact that the ethical responsibilities to respond to the risks of de-
20 identified data should not be borne by physicians alone. Respecting patient privacy and their
21 informed consent are responsibilities that physician member organizations and health care
22 institutions must take on because the risks to these rights that patients face within digital health
23 ecosystems radiate far beyond the patient–physician relationship to areas where individual
24 physicians have little influence.

25 26 RECOMMENDATIONS

27
28 In light of the challenges considered with regard to constructing a framework for holding
29 stakeholders accountable within digital health information ecosystems, the Council on Ethical and
30 Judicial Affairs recommends:

31 32 1. That the following be adopted:

33
34 Within health care systems, identifiable private health information, initially derived from and
35 used in the care and treatment of individual patients, has led to the creation of massive de-
36 identified datasets. As aggregate datasets, clinical data takes on a secondary promising use as a
37 means for quality improvement and innovation that can be used for the benefit of future
38 patients and patient populations. While de-identification of data is meant to protect the privacy
39 of patients, there remains a risk of re-identification, so while patient anonymity can be
40 safeguarded it cannot be guaranteed. In handling patient data, individual physicians thus strive
41 to balance supporting and respecting patient privacy while also upholding ethical obligations to
42 the betterment of public health.

43
44 When clinical data are de-identified and aggregated, their potential use for societal benefits
45 through research and development is an emergent, secondary use of electronic health records
46 that goes beyond individual benefit. Such data, due to their potential to benefit public health,
47 should thus be treated as a form of public good, and the ethical standards and values of health
48 care should follow the data and be upheld and maintained even if the data are sold to entities
49 outside of health care. The medical profession’s responsibility to protect patient privacy as well
50 as to society to improve future health care should be recognized as inherently tied to these

1 datasets, such that all entities granted access to the data become data stewards with a duty to
2 uphold the ethical values of health care in which the data were produced.

3
4 As individuals or members of health care institutions, physicians should:

- 5
6 (a) Follow existing and emerging regulatory safety measures to protect patient privacy;
7
8 (b) Practice good data intake, including collecting patient data equitably to reduce bias in
9 datasets;
10
11 (c) Answer any patient questions about data use in an honest and transparent manner to the
12 best of their ability in accordance with current federal and state legal standards.
13

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

- 16
17 (d) The high value that health care institutions place on protecting patient data;
18
19 (e) The reality that no data can be guaranteed to be permanently anonymized, and that risk of
20 re-identification does exist;
21
22 (f) How patient data may be used;
23
24 (g) The importance of de-identified aggregated data for improving the care of future patients.
25

26 Health care entities managing de-identified datasets, as health data stewards, should:

- 27
28 (h) Ensure appropriate data collection methods and practices that meet industry standards to
29 support the creation of high-quality datasets;
30
31 (i) Ensure proper oversight of patient data is in place, including Data Use/Data Sharing
32 Agreements for the use of de-identified datasets that may be shared, sold, or resold;
33
34 (j) Develop models for the ethical use of de-identified datasets when such provisions do not
35 exist, such as establishing and contractually requiring independent data ethics review
36 boards free of conflicts of interest and verifiable data audits, to evaluate the use, sale, and
37 potential resale of clinically-derived datasets;
38
39 (k) Take appropriate cyber security measures to seek to ensure the highest level of protection is
40 provided to patients and patient data;
41
42 (l) Develop proactive post-compromise planning strategies for use in the event of a data
43 breach to minimize additional harm to patients;
44
45 (m) Advocate that health- and non-health entities using any health data adopt the strongest
46 protections and seek to uphold the ethical values of the medical profession.
47

48 There is an inherent tension between the potential benefits and burdens of de-identified
49 datasets as both sources for quality improvement to care as well as risks to patient privacy. Re-
50 identification of data may be permissible, or even obligatory, in rare circumstances when done
51 in the interest of the health of individual patients. Re-identification of aggregated patient data

1 for other purposes without obtaining patients' express consent, by anyone outside or inside of
2 health care, is impermissible. (New HOD/CEJA Policy); and
3

- 4 2. That Opinion 2.1.1, "Informed Consent"; Opinion 3.1.1, "Privacy in Health Care"; Opinion
5 3.2.4, "Access to Medical Records by Data Collection Companies"; and Opinion 3.3.2,
6 "Confidentiality and Electronic Medical Records" be amended by addition as follows:
7

8 a. Opinion 2.1.1, Informed Consent
9

10 Informed consent to medical treatment is fundamental in both ethics and law. Patients have the
11 right to receive information and ask questions about recommended treatments so that they can
12 make well-considered decisions about care. Successful communication in the patient-physician
13 relationship fosters trust and supports shared decision making. Transparency with patients
14 regarding all medically appropriate options of treatment is critical to fostering trust and should
15 extend to any discussions regarding who has access to patients' health data and how data may
16 be used.
17

18 The process of informed consent occurs when communication between a patient and physician
19 results in the patient's authorization or agreement to undergo a specific medical intervention. In
20 seeking a patient's informed consent (or the consent of the patient's surrogate if the patient
21 lacks decision-making capacity or declines to participate in making decisions), physicians
22 should:
23

- 24 (a) Assess the patient's ability to understand relevant medical information and the implications
25 of treatment alternatives and to make an independent, voluntary decision.
26
27 (b) Present relevant information accurately and sensitively, in keeping with the patient's
28 preferences for receiving medical information. The physician should include information
29 about:
30
31 (i) the diagnosis (when known);
32
33 (ii) the nature and purpose of recommended interventions;
34
35 (iii) the burdens, risks, and expected benefits of all options, including forgoing treatment.
36
37 (c) Document the informed consent conversation and the patient's (or surrogate's) decision in
38 the medical record in some manner. When the patient/surrogate has provided specific
39 written consent, the consent form should be included in the record.
40

41 In emergencies, when a decision must be made urgently, the patient is not able to participate in
42 decision making, and the patient's surrogate is not available, physicians may initiate treatment
43 without prior informed consent. In such situations, the physician should inform the
44 patient/surrogate at the earliest opportunity and obtain consent for ongoing treatment in
45 keeping with these guidelines. (Modify HOD/CEJA Policy)
46

47 b. Opinion 3.1.1, Privacy in Health Care
48

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

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

5
6 Physicians must seek to protect patient privacy in all settings to the greatest extent possible and
7 should:

- 8
9 (a) Minimize intrusion on privacy when the patient's privacy must be balanced against other
10 factors.
11
12 (b) Inform the patient when there has been a significant infringement on privacy of which the
13 patient would otherwise not be aware.
14
15 (c) Be mindful that individual patients may have special concerns about privacy in any or all
16 of these areas.
17
18 (d) Be transparent with any inquiry about existing privacy safeguards for patient data but
19 acknowledge that anonymity cannot be guaranteed and that breaches can occur
20 notwithstanding best data safety practices. (Modify HOD/CEJA Policy)
21

22 c. Opinion 3.2.4, Access to Medical Records by Data Collection Companies
23

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

29
30 Information gathered and recorded in association with the care of a patient is confidential.
31 Patients are entitled to expect that the sensitive personal information they divulge will be used
32 solely to enable their physician to most effectively provide needed services. Disclosing
33 information to third parties for commercial purposes without consent undermines trust, violates
34 principles of informed consent and confidentiality, and may harm the integrity of the patient-
35 physician relationship.

36
37 Physicians who propose to permit third-party access to specific patient information for
38 commercial purposes should:

- 39
40 (a) Only provide data that has been de-identified.
41
42 (b) Fully inform each patient whose record would be involved (or the patient's authorized
43 surrogate when the individual lacks decision-making capacity) about the purpose(s) for
44 which access would be granted.
45

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

- 48
49 (c) Obtain the consent of the patient (or authorized surrogate) to permit access to the patient's
50 medical record.

1 (d) Prohibit access to or decline to provide information from individual medical records for
2 which consent has not been given.

3
4 (e) Decline incentives that constitute ethically inappropriate gifts, in keeping with ethics
5 guidance.

6
7 Because de-identified datasets are derived from patient data as a secondary source of data for
8 the public good, health care professionals and/or institutions who propose to permit third-party
9 access to such information have a responsibility to establish that any use of data derived from
10 health care adhere to the ethical standards of the medical profession. (Modify HOD/CEJA
11 Policy)

12
13 d. Opinion 3.3.2, Confidentiality and Electronic Medical Records

14
15 Information gathered and recorded in association with the care of a patient is confidential,
16 regardless of the form in which it is collected or stored.

17
18 Physicians who collect or store patient information electronically, whether on stand-alone
19 systems in their own practice or through contracts with service providers, must:

20
21 (a) Choose a system that conforms to acceptable industry practices and standards with respect
22 to:

23
24 (i) restriction of data entry and access to authorized personnel;

25
26 (ii) capacity to routinely monitor/audit access to records;

27
28 (iii) measures to ensure data security and integrity; and

29
30 (iv) policies and practices to address record retrieval, data sharing, third-party access and
31 release of information, and disposition of records (when outdated or on termination of
32 the service relationship) in keeping with ethics guidance.

33
34 (b) Describe how the confidentiality and integrity of information is protected if the patient
35 requests.

36
37 (c) Release patient information only in keeping with ethics guidance for confidentiality and
38 privacy. (Modify HOD/CEJA Policy); and

39
40 3. That the remainder of this report be filed.

Fiscal Note: Less than \$500

REFERENCES

1. Ruotsalainen P, Blobel B. Health information systems in the digital health ecosystem—problems and solutions for ethics, trust and privacy. *Int J of Envir Res and Pub health* 2020;17(9):3006.
2. McGraw D, Mandl KD. Privacy protections to encourage use of health-relevant digital data in a learning health system. *NPJ dig med* 2021;4(1):2.
3. Floridi L, Cath C, Taddeo M. Digital ethics: its nature and scope. *The 2018 yearbook of the digital ethics lab* 2019:9-17.
4. Data monetization in healthcare market size report, 2030. In: *Data Monetization In Healthcare Market Size Report, 2030*. <https://www.grandviewresearch.com/industry-analysis/data-monetization-healthcare-market-report>.
5. Larson DB, Magnus DC, Lungren MP, Shah NH, Langlotz CP. Ethics of using and sharing clinical imaging data for artificial intelligence: a proposed framework. *Radiology* 2020;295(3):675-82.
6. Barocas S, Nissenbaum H. Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement* 2014;1:44-75.
7. Price WN II, Cohen IG. Privacy in the age of medical big data. *Nat Med* 2019;25:37–43.
8. Raghupathi W, Raghupathi V, Saharia A. Analyzing Health Data Breaches: A Visual Analytics Approach. *AppliedMath* 2023;3(1):175-99.
9. Hansson MG, Lochmüller H, Riess O, Schaefer F, Orth M, Rubinstein Y, Molster C, Dawkins H, Taruscio D, Posada M, Woods S. The risk of re-identification versus the need to identify individuals in rare disease research. *Eur J Hum Genet* 2016;24(11):1553-1558. doi:10.1038/ejhg.2016.52.
10. Nissenbaum, H. Respecting context to protect privacy: why meaning matters. *Sci Eng Ethics* 2018;24:831–52.
11. Nissenbaum H. Privacy as contextual integrity. *Wash. L. Rev* 2004;79:119-158.
12. Weng CY. Data Accuracy in Electronic Medical Record Documentation. *JAMA Ophthalmol* 2017;135(3):232–233. doi:10.1001/jamaophthalmol.2016.5562
13. Pew. Enhancing patient matching is critical to achieving full promise of digital health records: Accurately linking individuals with their health records essential to improving care. *Pew Trust Report* October 2, 2018. <https://www.pewtrusts.org/en/research-and-analysis/reports/2018/10/02/enhanced-patient-matching-critical-to-achieving-full-promise-of-digital-health-records>
14. Boyd AD, Gonzalez-Guarda R, Lawrence K, Patil CL, Ezenwa MO, O'Brien EC, Paek H, Braciszewski JM, Adeyemi O, Cuthel AM, Darby JE. Equity and bias in electronic health records data. *Contemp Clinic Trials* 2023;130:107238.
15. Boyd AD, Gonzalez-Guarda R, Lawrence K, Patil CL, Ezenwa MO, O'Brien EC, Paek H, Braciszewski JM, Adeyemi O, Cuthel AM, Darby JE. Potential bias and lack of generalizability in electronic health record data: reflections on health equity from the National Institutes of Health Pragmatic Trials Collaboratory. *J of the Am Medl Informat Ass* 2023:ocad115.
16. Khurshid S, Reeder C, Harrington LX, Singh P, Sarma G, Friedman SF, Di Achille P, Diamant N, Cunningham JW, Turner AC, Lau ES. Cohort design and natural language processing to reduce bias in electronic health records research. *NPJ Digital Med* 2022;5(1):47.
17. NIH. Informed consent for secondary research with data and biospecimens: Points to consider and sample language for future use and/or sharing. *NIH Office of Science Policy Office of Extramural Research* May 2020. <https://osp.od.nih.gov/wp-content/uploads/Informed-Consent-Resource-for-Secondary-Research-with-Data-and-Biospecimens.pdf>
18. Skahill E, West DM. Why hospitals and healthcare organizations need to take cybersecurity more seriously. *Brookings* August 9, 2021. <https://www.brookings.edu/articles/why-hospitals-and-healthcare-organizations-need-to-take-cybersecurity-more-seriously/>

19. Winter JS, Davidson E. Big Data Governance of personal health information and challenges to Contextual Integrity. *The Information Society* 35:36–51. doi: 10.1080/01972243.2018.1542648
20. Allen C, Des Jardins TR, Heider A, et al. Data Governance and data sharing agreements for community-wide health information exchange: Lessons from the Beacon Communities. *eGEMs (Generating Evidence & Methods to improve patient outcomes)* 2:5. doi: 10.13063/2327-9214.1057

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: [new content sets out context of guidance explicitly]

- (a) *Only provide data that has been de-identified. [new content consistent with 3.1.2]*
- (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: [new content sets out context of guidance explicitly]

- (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. [new content makes expectation explicit]*
- (e) Decline incentives that constitute ethically inappropriate gifts, in keeping with ethics guidance.

AMA Principles of Medical Ethics: I,II,IV

5. PHYSICIAN ADVISORY OR REFERRAL SERVICES BY TELEPHONE*

HOUSE ACTION: FILED

Telephone advisory services can be a helpful source of medical information for the public. Often, people are not sure where to turn for information of a general medical nature or do not have easy access to other sources of information. Individuals also may be embarrassed about directly bringing up certain questions with their physicians. Although telephone advisory services can only provide limited medical services, they can be a useful complement to more comprehensive services, if used properly.

Any telephone advisory service should employ certain safeguards to prevent misuse. For example, the physician responding to the call should not make a clinical diagnosis. Diagnosis by telephone is done without the benefit of a physical examination or even a face-to-face meeting with the caller. Critical medical data may be unavailable to the physician. Physicians who respond to callers should therefore act within the limitations of telephone services and ensure that callers understand the limitations of the services. Under no circumstances should medications be prescribed.

Physicians who respond to the calls should elicit all necessary information from the callers. When callers are charged by the minute, they may try to hurry their calls to limit their costs. As a result, important information may not be disclosed to the physician. Physicians should also ensure that callers do not incur large bills inadvertently or without understanding the billing system.

Physician referral services can also offer important information to the public. Referral services are often provided by medical societies, hospitals and for-profit entities. To ensure that the service bases its recommendation on medically legitimate considerations rather than the likelihood of being paid by the physician, when the service charges physicians a fee to participate, physicians should not pay the service per referral. Also, callers should be told how the list is created. For example, callers should be informed whether the list includes physicians who pay a flat fee to be listed, members of a particular hospital staff or medical society, or physicians who meet some general quality-based criteria.

While these safeguards are described as applying primarily to telephone services, they should be considered equally applicable to any other communication media, such as radio, television or computer, in which the physician and patient do not meet face-to-face.

(The Physician Advisory or Referral Services by Telephone Opinion will appear in the next edition of Current Opinions with Annotations as Opinion 5.025 and is derived from Principles I, IV and VI of the Principles of Medical Ethics.)

6. DISCLOSURE OF RECORDS TO DATA COLLECTION COMPANIES*

HOUSE ACTION: FILED

Data-collection from computerized or other patient records for marketing purposes raises serious ethical concerns. In some cases, firms have sought to amass information on physicians' prescribing practices on behalf of pharmaceutical houses for marketing purposes. Often, physicians are offered incentives such as computer hardware and software packages in return for agreeing to such an arrangement. They may be told that data-collecting software does not capture patients' names.

These arrangements may violate principles of informed consent and patient confidentiality. Patients divulge information to their physicians only for purposes of diagnosis and treatment. If other uses are to be made of the

information, patients must give their permission after being fully informed about the purpose of such disclosures. If permission is not obtained, physicians violate patient confidentiality by sharing specific and intimate information from patients' records with commercial interests.

Arrangements of this kind may also violate Opinion 8.061 on gifts to physicians from industry.

Finally, these arrangements may harm the integrity of the patient-physician relationship. The trust that is fundamental to this relationship is based on the principle that the physicians are the agents first and foremost of their patients.

(The Disclosure of Records to Data Collection Companies Opinion will appear in the next edition of Current Opinions with Annotations as Opinion 5.075 and is derived from Principles I, II and IV of the Principles of Medical Ethics.)

7. PROFESSIONAL COURTESY*

HOUSE ACTION: FILED

Professional courtesy refers to the provision of medical care to physician colleagues or their families free of charge or at a reduced rate. While professional courtesy is a long-standing tradition in the medical profession, it is not an ethical requirement. Physicians should use their own judgment in deciding whether to waive or reduce their fees when treating fellow physicians or their families. Physicians should be aware that accepting insurance payments while waiving patient co-payments may violate Opinion 6.12.

(The Professional Courtesy Opinion will appear in the next edition of Current Opinions with Annotations as Opinion 6.13 and is derived from Principles II and IV of the Principles of Medical Ethics.)

8. RETENTION OF MEDICAL RECORDS*

HOUSE ACTION: FILED

Physicians have an obligation to retain patient records which may reasonably be of value to a patient. The following guidelines are offered to assist physicians in meeting their ethical and legal obligations:

1. Medical considerations are the primary basis for deciding how long to retain medical records. For example, operative notes and chemotherapy records should always be part of the patient's chart. In deciding whether to keep certain parts of the record, an appropriate criterion is whether a physician would want the information if he or she were seeing the patient for the first time.
2. If a particular record no longer needs to be kept for medical reasons, the physician should check state laws to see if there is a requirement that records be kept for a minimum length of time. Most states will not have such a provision. If they do, it will be part of the statutory code or state licensing board.
3. In all cases, medical records should be kept for at least as long as the length of time of the statute of limitations for medical malpractice claims. The statute of limitations may be three or more years, depending on the state law. State medical associations and insurance carriers are the best resources for this information.