REPORT 7 OF THE COUNCIL ON MEDICAL SERVICE (A-24)
Ensuring Privacy in Retail Health Care Settings
(Reference Committee A)

EXECUTIVE SUMMARY

At the 2023 Annual Meeting, the House of Delegates adopted Policy H-315.960, which asks our American Medical Association to "study privacy protections, privacy consent practices, the potential for data breaches, and the use of health data for non-clinical purposes in retail health care settings."

The growth in retail health care clinics makes them a significant player in the $4 trillion US health care system. Retail health care is a term used to describe two discrete models of care: 1) walk-in clinics that provide treatment from employed non-physician practitioners; or 2) services that connect patients with participating online clinics. This distinction is important as it has implications in deciphering responsibilities of covered entities and business associates, respectively.

While the Health Insurance Portability and Accountability Act (HIPAA) has been in place since 1996, misconceptions have muddied the waters around what is and is not a covered entity or business associate, and what is or is not protected health information (PHI). Furthermore, there is confusion surrounding retail health care companies' HIPAA status, as they require patients to read and comprehend several documents together in order to understand their rights. For these reasons, the Council has developed recommended guardrails surrounding retail health care companies' handling of PHI.

REPORT OF THE COUNCIL ON MEDICAL SERVICE

CMS Report 7-A-24

Subject: Ensuring Privacy in Retail Health Care Settings

Presented by: Sheila Rege, MD, Chair

Referred to: Reference Committee A

At the 2023 Annual Meeting, the House of Delegates adopted Policy H-315.960, which asks our American Medical Association (AMA) to "study privacy protections, privacy consent practices, the potential for data breaches, and the use of health data for non-clinical purposes in retail health care settings." Testimony at the 2023 Annual Meeting regarding the resolution was unanimously supportive, highlighting a strong commitment to patient privacy as well as expansion to include health data for nonclinical purposes and all retail health care settings. This report focuses on current privacy practices in retail health care settings, highlights AMA advocacy efforts and essential policy, and presents new policy recommendations.

BACKGROUND

As of March 2023, there were 1,801 active retail health care clinics in 44 states, predominantly in major metropolitan areas. While only two percent of retail health care clinics are in rural areas, CVS Health owns half of those as well as 63 percent of all retail health care clinics. Kroger Health is the second largest, at 12 percent market share, with more than 220 retail clinics in 35 states, and Walgreens is the third largest at eight percent.[1] Other participants include Walmart, Amazon, Best Buy, and Dollar General. Most retail clinics are in the Southeast and the Midwest, which account for 62 percent of locations. Nearly half (49.1 percent) of all retail clinics are concentrated in seven states: Texas, Florida, Ohio, California, Georgia, Illinois, and Tennessee, which can be attributed to population density. Retail health care clinics have seen a 202 percent increase in utilization from 2021 to 2022,[2] which is a greater growth percentage than seen by urgent care centers, primary care practices, and hospital emergency departments. While retail health care has been around since the early 2000s, it is now a significant player in the $4 trillion U.S. health care system.[3] Retailers' substantial financial resources and far reach allow them to push a customized consumer experience focused on convenience and driven by digital health products, permitting them to get closer to consumers as e-commerce erodes their traditional business. Companies such as CVS Health, Walgreens, Costco, and Amazon continue to expand their services, pulling together different technology-enabled services such as urgent, primary, home, and specialty care along with pharmacy and, in some cases, full integration with an insurer, prompting anti-trust and privacy concerns.

A 2022 AMA survey found that while 92 percent of people believe that privacy of their health data is a right, most are unclear about the rules relevant to their privacy. The AMA is concerned that health data are increasingly vulnerable and has called for regulations for an individual's right to control, access, and delete personal data collected about them. The issue is further exacerbated by the Supreme Court's decision to overturn *Roe v. Wade*, which challenges the right to privacy by

potentially enabling law enforcement to gain access to health data related to abortion care and pregnancy.[4] As such, the AMA has outlined five privacy principles for a national privacy framework, including:

- Individual rights
- Equity
- Entity responsibility
- Applicability
- Enforcement

SNAPSHOT OF CURRENT RETAIL HEALTH CARE MARKET

Walmart is reportedly in negotiations with ChenMed, which touts itself as "family-owned, family-oriented organization committed to bringing superior health care to moderate-to-low-income seniors." Walgreens recently announced that it is teaming up with technology company Pearl Health, which has a platform to enable value-based care. The collaboration will merge Pearl's operating system capabilities with Walgreens' care delivery assets, allowing Walgreens to function as a management services organization for physicians and hospitals. Costco is partnering with the online platform Sesame, which operates outside of insurance networks in order to cater to patients with high-deductible health plans and to the uninsured. Costco will be able to offer same-day telehealth primary care visits for $29, as well as video prescription refills, mental health consults, and in-person visits for urgent care, among other services. In 2018, Amazon acquired start-up PillPack, which later became Amazon Pharmacy. In November 2022, the company launched Amazon Clinic, a virtual health service that provides users with 24/7 access to physicians and nurse practitioners on Amazon's website and mobile application (app). In February 2023, Amazon purchased One Medical, which is a membership-based, tech-integrated primary care platform. Amazon is now piloting delivery of medications via drone, airlifting certain common medicines to homes within 60 minutes.[5] Most recently, Amazon introduced its Health Conditions Programs, an initiative that enables customers to discover digital health benefits to help manage chronic conditions such as diabetes and hypertension. Customers answer questions to determine if their insurance covers a program and if they are clinically eligible for that program, for which they gain access to specific services (e.g., virtual health coaching) and devices (e.g., continuous glucose monitors) covered by their plan. CVS Health owns Aetna, Oak Street Health, and Caremark. In December 2017, CVS announced its merger with Aetna, representing the biggest health care merger in US history, involving both a horizontal and a vertical merger. While the AMA led advocacy efforts to block the union, it was eventually approved.

FEDERAL DATA PRIVACY LAWS

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, establishing a comprehensive set of standards for protecting sensitive patient health information. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable patient health information (collectively defined as "protected health information" or PHI). It requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

PHI is any individually identifiable health information created, received, maintained, or transmitted by a covered entity or business associate that:

- Relates to the past, present, or future physical or mental health or condition of an individual,
- The provision of health care to an individual, or
- The past, present, or future payment for the provision of health care to an individual.

The United States does not have a federal law that affirms who owns medical records. Under HIPAA, patients have the right to access data medical information in their medical records. The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization. The HIPAA Privacy Rule also gives individuals rights over their PHI, including rights to examine and obtain a copy of their health records, to direct a covered entity to transmit to a third-party an electronic copy of their protected health information in an electronic health record, and to request corrections. It applies to all entities that fall within the definition of a "covered entity," which includes health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. Third-party organizations that provide a service for or on behalf of a covered entity are referred to as "business associates" when the service they provide requires that the covered entity disclose PHI to them; common examples of a business associate are a claims processing entity or appointment scheduling service. All business associates are required to comply with HIPAA privacy protections to the same extent as the covered entity for which the services are performed.

Retail health care is a term used to describe two discrete models of care: 1) walk-in clinics that provide treatment from employed non-physician practitioners (e.g., CVS Minute Clinic); or 2) services that connect patients with participating online clinics (e.g., Amazon Clinic). This distinction is important as it has implications in deciphering responsibilities of covered entities (e.g., CVS Affiliated Covered Entity, which designates itself as a single covered entity made up of covered entities and health care providers owned or controlled by CVS) and business associates, respectively. In order to help health care providers and organizations determine their HIPAA status, the Centers for Medicare & Medicaid Services has developed a *Covered Entity Decision Tool*.

While HIPAA has been in place since 1996, misconceptions persist regarding what is and is not a covered entity or business associate, and what is or is not PHI. Fortunately, in this regard, the HIPAA regulations have not changed in 10 years, since the 2013 HIPAA and Health Information Technology for Economic Clinical Health Act (HITECH) Omnibus Rule. Therefore, the following still hold true:

- A legally compliant business associate (BA) status can only be achieved by signing a BA agreement (BAA) with a covered entity (CE).
- The minimum terms of each business association agreement (BAA) are mandated by regulations, which have also not changed since 2013.
- The Privacy Rule provides that a BAA must require a BA to return all PHI to the CE or destroy the PHI at the termination of the BAA where feasible.

Legally, the HIPAA Privacy Rule applies to covered entities and business associates. Covered entities are also responsible for guaranteeing their business associates are safeguarding PHI under contract. The contract between the covered entity and its business associate must be HIPAA compliant. If a business associate breaches its contract, then it is up to the covered entity to correct that breach or terminate the contract. In the event of a loss of PHI by a BA, a CE can be responsible for their loss of data.

Health care data that are not created, received, maintained, or transmitted by a CE or BA are referred to as "health care adjacent data" and are not protected by the HIPAA Privacy Rule, nor subject to the safeguards of the HIPAA Security Rule. The HIPAA Security Rule requires CEs and BAs to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronically stored PHI (ePHI). However, health care entities that collect, use, store, and share personal health data from digital health platforms, apps, and other similar software programs (e.g., Fitbit) are not CEs or BAs and are, therefore, beyond the reach of HIPAA. These apps may be held legally accountable by federal regulators for inappropriate disclosures or data breaches by the Federal Trade Commission (FTC).

RETAIL HEALTH CARE ORGANIZATIONS' HIPAA STATUS

In some cases, there is confusion regarding a retail health care company's HIPAA status, requiring patients to read and comprehend several documents together in order to understand their rights. Determining which organizations HIPAA protections apply is a complex question, as HIPAA regulates not only the three types of covered entities (health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with a covered transaction), but also their business associates, which can be difficult for the layperson to identify. Additionally, while retail health companies often contend that they have stringent customer privacy policies, they may still require customers to sign away some data protection rights. For example, Amazon's privacy page explains that the Clinic is not a health care provider – in other words, it is not a HIPAA covered entity. It goes on to explain that Amazon Clinic is a service provider to health care providers – thereby classifying it as a HIPAA business associate, retaining patient PHI in order to "coordinate health care services and update customer information to facilitate services from other providers." However, the Amazon Clinic HIPAA Authorization webpage states that it is "in compliance with federal privacy laws, including HIPAA" and includes FAQs that reference its use of "HIPAA compliant technology." The challenge is that the Amazon Clinic HIPAA Authorization needs to be read together with the intricate terms of several other Amazon legal policies, including its Amazon Clinic Terms of Use, Amazon.com Conditions of Use, and Amazon.com Privacy Notice in order for patients to understand all their privacy rights. While retail health companies contend that they have stringent customer privacy policies, there have been accounts of companies requiring customers to sign away some data protection rights. In May 2023, the *Washington Post* reported that when enrolling for Amazon Clinic, users are required to provide consent to allow the use and disclosure of their PHI. The form that patients are asked to complete states that after providing consent, Amazon will be authorized to have access to the complete patient file, may re-disclose information contained in that file, and that the information disclosed will no longer be subject to HIPAA Rules.[6] While the terms are voluntary, individuals have no option of using Amazon Clinic if they do not agree to the terms and conditions.[7] The fundamental problem is that once patients agree to the Amazon Clinic authorization, they agree their health information may no longer be protected by HIPAA.[8] How retail health care companies decide to manipulate data and use it may not become apparent for many years.

CONSUMER PROTECTION & PRIVACY LAWS

Retail health care organizations that electronically transmit standard transactions (e.g., payment, enrollment, eligibility) are covered entities subject to HIPAA. They are also subject to other consumer protection and privacy laws for non-HIPAA covered entities. Privacy rights are included in the FTC's authority to protect consumers from deceptive or unfair business practices. The FTC Health Breach Notification Rule specifically applies to non-HIPAA covered entities who are required to notify their customers, the FTC, and, in some instances, the media if there is a breach of unsecured, individually identifiable health information.[9]

The State of Washington recently passed a privacy-focused law to protect PHI that falls outside HIPAA. The My Health My Data Act makes it illegal to sell or offer to sell PHI without first obtaining authorization from the consumer.[10] Several other states (i.e., California, Colorado, Connecticut, Utah, and Virginia) have enacted general privacy laws with varying applicability to retail health care companies. The latter laws include various exemptions for PHI, HIPAA de-identified information, health care providers, HIPAA covered entities, HIPAA business associates, and non-profits. While all of the latter laws exempt PHI, retail health care companies may have obligations under these laws with respect to other personal information, such as website data.[11]

RETAIL HEALTH PRIVACY PROTECTIONS & CONSENT PRACTICES

In a privacy notice, retail health care companies outline how HIPAA allows them to use and share PHI for treatment, payment, and health care operations. Their privacy notices also describe the circumstances where uses and disclosures of PHI do not require patient approval, including certain uses and disclosures by business associates (i.e., service providers to health care providers), designated patient caregivers, workers' compensation claims, law enforcement, judicial or administrative proceedings, public health purposes, health oversight activities (e.g., audits), institutional review board-approved research, coroners, medical examiners and funeral directors, organ procurement organizations, correctional institutions, and military/national security activities. Retail health care companies are prohibited from disclosing PHI for purposes other than those described in their notices or for marketing purposes of any kind without written patient consent. Additionally, patients are notified that they may revoke their approval at any time, although most companies require submission of formal written notice, explaining that revocation cannot undo any use or sharing of PHI that has already happened based on previously granted permission.

It is important to note that Amazon Clinic is not required to secure any additional waiver or "authorization" from prospective patients in order for Amazon Clinic to provide the services it promises to perform in regard to matching the patient with an available medical provider. This type of scheduling and care coordination is one aspect of "health care operations" under HIPAA, and falls within the Treatment, Payment, and Health Care Operations permissible disclosures under HIPAA, for which no patient authorization is required.* Per Department of Health & Human Services-Office of Civil Rights (OCR) guidance, "A business associate agreement may authorize a business associate to make uses and disclosures of PHI the covered entity itself is permitted by the HIPAA Privacy Rule to make. See 45 C.F.R. § 164.504(e)." Patients are asked to sign a voluntary Amazon Clinic HIPAA authorization. The superfluous nature of Amazon's HIPAA authorization form seems to be a tactic aimed at obtaining valuable PHI. This strategy not only allows Amazon access to use and disclose the PHI relevant to its patient matching services, it secures Amazon's ability to collect, use, and disclose each patient's "complete patient file" – far exceeding the amount of information needed to match a patient with a medical provider.

---

* See 45 C.F.R. §164.506(a) Standard: Permitted uses and disclosures. A covered entity may use or disclose protected health information for treatment, payment, or health care operations provided that such use or disclosure is consistent with other applicable requirements of this subpart. (emphasis in original). See also, "Health care operations are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination . . ." (emphasis in original) https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=Health %20care %20operations%20are%20any,c)%20conducting%20or%20arranging%20for. See finally, 45 C.F.R. §164.506 (c)(2): "A covered entity may disclose protected health information for treatment activities of a health care provider." In the case of Amazon Clinic, Amazon discloses patient PHI to its participating providers to facilitate the patient's treatment, in addition to care coordination.

The breadth of retail health care companies' coast-to-coast networks can amplify privacy concerns. In December 2023, the Senate Committee on Finance found that eight of the nation's largest pharmacy chains had routinely turned over customers' PHI to law enforcement agencies, even without a warrant, concluding that, "these companies' privacy practices vary widely, in ways that seriously impact patient privacy." None of the companies required a warrant before turning over requested data, as HIPAA does not require law enforcement to obtain a warrant or judge-issued subpoena before they make a lawful request for records containing PHI.

ETHICAL & COMPETITIVE CONSIDERATIONS

The investment banking industry utilizes a virtual information barrier between those who have material, non-public information and those who do not, to prevent conflicts of interest, sometimes referred to as an "ethical wall" or privacy wall. The legal services industry utilizes a similar firewall to protect clients by restraining access to information in order to prevent conflicts of interest among law firm attorneys who may have represented a now adverse party in their prior legal work. Establishing a privacy wall between the health business and non-health business of retail health care companies could eliminate sharing of identifiable PHI or re-identifiable PHI for uses not directly related to patients' medical care.

Amazon's acquisition of One Medical is a cautionary example. The union allows Amazon to collect a large cache of PHI to further cement its dominance as an online intermediary for goods and services. Amazon's cross-industry reach allows it to use data to develop detailed insights about individuals, without much risk of violating privacy laws. In order to protect the privacy of patients, it will be important for Amazon to commit to having a privacy wall between its patient data and its other areas. Amazon notes that it "will never share One Medical PHI outside of One Medical for advertising or marketing purposes of other Amazon products and services without clear permission from the customer."[12] However, Amazon makes patients accept its conditions of use prior to treatment, which signs away their PHI protections.[13] The combination of a vast product distributor and marketer with sensitive PHI sets the stage for unfettered targeted advertising.

The implications of horizonal-vertical health care mergers, such as the one between CVS and Aetna, cannot be overlooked. An AMA evidence-based analysis showed how the merger would reduce competition in five key health care markets: Medicare Part D; health insurance; pharmacy benefit management; retail pharmacy; and specialty pharmacy, leading to higher premiums and lower-quality insurance products. Such mergers may lead to increased access to PHI, leveraging data on individual biology, medical history, level of well-being, shopping habits, sleep hygiene, nicotine consumption, and exercise routines to shape patients' digital health IDs. This can allow health insurers to reduce their risks and, therefore, their costs by restricting access to health care services for high-risk patients and vulnerable populations.

POTENTIAL FOR DATA BREACHES

On February 21, 2024, a cyberattack against UnitedHealth Group's Change Healthcare disrupted operations for physicians, hospitals, insurers, and pharmacies. Change Healthcare uses Amazon Web Services (AWS) to submit and process insurance claims, handling close to 14 billion transactions a year. As of March 1, 2024, Change Healthcare reported that it was working with Microsoft and AWS to perform an additional scan of its cloud environment. This breach highlights the potential for cyberattacks to affect patient privacy in the retail health care setting.

The four most common reasons for data breaches include cyberattacks, unauthorized disclosure, theft, and improper disposal of PHI.[14] As retail health care companies expand their reach, the risk

of a data breach increases exponentially, especially if they fail to establish the technical controls, training, and employee sanctions necessary to isolate retail health care business from other lines of business. Legal and technical firewalls are essential in preventing retail health care data breaches because they serve as the first line of defense in protecting ePHI from external threats such as hacking, as well as unauthorized or unintended disclosures across business lines.

Once a covered entity knows or by reasonable diligence should have known (referred to as the "date of discovery") that a breach of PHI has occurred, the entity has an obligation to notify the relevant parties "without unreasonable delay" or up to 60 calendar days following the date of discovery, even if upon discovery the entity was unsure as to whether PHI had been compromised. If the breach involves the unsecured PHI of more than 500 individuals, a covered entity must notify a prominent media outlet serving the state or jurisdiction in which the breach occurred, in addition to notifying the Department of Health & Human Services (HHS). For breaches involving fewer than 500 individuals, covered entities are permitted to maintain a log of the relevant information and notify HHS within 60 days after the end of the calendar year via the HHS website. Additionally, covered entities may offer affected individuals free identity restoration services or credit reports for a defined period of time. While such offerings are well intended, they do not necessarily allow reparations commensurate with the degree of harm experienced by the affected individuals.

USE OF HEALTH DATA FOR NON-CLINICAL PURPOSES

Secondary use of PHI includes activities such as analysis, research, quality and safety measurement, public health, payment, physician accreditation, marketing, risk stratifying to limit care to high-risk patients and vulnerable populations, and other business applications. As retail health care companies continue to expand their reach, the potential for them to use PHI for non-clinical purposes grows. The FTC sent a letter to Amazon in anticipation of its acquisition of One Medical, reminding it of the obligation to protect sensitive health information and inquiring as to how the integrated entity will use One Medical PHI for purposes beyond the provision of health care. Amazon's acquisition of One Medical was finalized in February 2023 without a regulatory challenge. While the FTC could file a lawsuit to unwind the transaction in the future, experts agree that if regulators had found a reason to block the deal, they already would have. Granting retail health care companies enormous tranches of PHI is viewed by some as a mistake, given that loopholes exist in every legal framework.

THE ROLE OF AUGMENTED INTELLIGENCE IN DATA PRIVACY

De-identifying PHI enables HIPAA covered entities to share health data for large-scale medical research studies, policy assessments, comparative effectiveness studies, and other studies and assessments without violating the privacy of patients or requiring authorizations to be obtained from each patient prior to data being disclosed. Once PHI is de-identified and theoretically can no longer be traced back to an individual, it is no longer protected by the HIPAA Privacy Rule.[15] HIPAA-compliant de-identification of PHI is possible using one of two methods – Safe Harbor or Expert Determination. While neither method will remove all risk of re-identification of patients, both can reduce risk. In essence, almost all de-identified PHI is re-identifiable.

A covered entity may assign a code or other means of record identification to allow information de-identified to be re-identified by the covered entity. However, as long as the covered entity does not use or disclose the code or other means of record identification for any other purpose or does not disclose the mechanism for re-identification, they remain compliant with HIPAA.

The complexity and rise of data in health care means that augmented intelligence (AI) will increasingly be applied within the field. Several types of AI are already employed by payers, health plans, and life sciences companies. At the present time, the key categories of applications involve diagnosis and treatment recommendations, patient engagement and adherence, and administrative activities.[16] Health care adjacent data, such as data collected by wearables and health care applications, are commonly transmitted to an AI-driven health care solution – for example, for the early diagnosis of a heart condition. Accordingly, there is rising concern about the ability of AI to facilitate the re-identification of PHI with relative ease. AI algorithms are sophisticated enough to "learn" new strategies from data, such as how to discern patterns in the data. Through this detection, an algorithm may be able to effect PHI re-identification. The HIPAA Privacy Rule outlines specific requirements to adhere to when de-identifying health data, but there is currently no standardized approach for using de-identified data or validating best practices. While current laws do not address the role AI might play in data privacy, regulators are continually enacting and revising their policies, such as the European Union's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA). Under the GDPR, there must be a legal basis for collecting personal data, while the CCPA requires that users have the ability to opt out of any personal information collection practices. At the federal level, National Institute of Standards and Technology AI Standards are currently under development, while the Government Accountability Office report, Artificial Intelligence in Health Care provides guidance for future legislation. In the interim, AI vendors and software developers are advised to follow the Xcertia mHealth Guidelines, which align with many of HIPAA's standards and are backed by the AMA, one of the founding members. The Joint Commission recently launched the Responsible Use of Health Data Certification (RUHD), a voluntary program aimed at providing health care entities with an objective evaluation of how well they maintain health data privacy best practices in their secondary use of data for endeavors such as operations improvement or AI development. The RUHD will evaluate whether an organization de-identifies data in accordance with HIPAA, whether it has established a governance structure for the use of de-identified data, and how the organization communicates with key stakeholders about the secondary use of de-identified data. The AMA has also recently created a set of AI Principles which identify and advocate for enhanced protections for de-identified data when used in conjunction with generative AI and large language models.

ROADBLOCKS TO PRIVACY PROTECTION

As HIPAA only covers CEs and BAs, concerns arise in the regulation of entities currently beyond the scope of HIPAA, such as digital health platforms, apps, and other similar software programs that collect, use, store, and share personal health data. Under federal law there is no floor – no minimum threshold at all – for an organization's privacy policy. Thus, any health app or digital health platform can word their stated privacy policy in a weak, evasive, easy-to-comply-with manner that will sound reassuring to the consumers who choose to read it. Unfair and deceptive acts and practices affective commerce are a required basis of an FTC action. This is in stark contrast to the HIPAA Notice of Privacy Practices, which must include specific representations as to a CE's privacy practices.

Entities such as Amazon Clinic have taken a savvy approach by positioning themselves as BAs and thus subject to HIPAA, which reassures consumers. Amazon Clinic's BA status appears to have been achieved by entering into a BAA with each of the medical providers (i.e., CEs) who participate with Amazon Clinic. Amazon Clinic collects data from consumers and matches them with the Clinic's participating providers. Amazon is able to avoid most of the compliance burden and privacy protections that HIPAA requires of BAs, by requiring consumers to click through a screen whereby they effectively waive their HIPAA protections. Under HIPAA, a BA may not use or disclose PHI in a manner that would violate the Privacy Rule if done by the CE, but HIPAA

does allow patients to effectively waive their rights against disclosure by the CE by giving an authorization, which is how Amazon characterizes its waiver/click-through screen. While amending HIPAA to provide that BAs may not get a waiver from consumers might be helpful, sophisticated companies such as Amazon would likely devise a strategy so the patient "authorization for disclosure" appears to come from the medical provider, and patient authorizations to disclose their PHI are a necessary feature of HIPAA. When patients sign up for treatment through Amazon Clinic, they also authorize all those involved (physicians, pharmacies, laboratories) to share their PHI with Amazon. Amazon then has the right to "retain, use, and disclose" PHI to facilitate services from "other providers." It is unclear who these other providers are, leading some to believe it could include businesses looking to target patients with ads related to their condition. A substantial hurdle to privacy protection seems to be the willingness of consumers to click through screens.

CHALLENGING PRIVACY ROADBLOCKS

To ensure robust privacy protections, the Council believes that retail health care companies should be prohibited from utilizing "clickwrap" agreements, which are online agreements where the user indicates their acceptance by clicking a button or checking a box that states, "I agree." While the purpose of a clickwrap agreement is to digitally capture acceptance of a contract, they permit patients to access a service without specific affirmative consent to data sharing. Common uses include asking website visitors to acknowledge that the website they are visiting uses cookies, installing a mobile app, or connecting to a wireless network.

The Council also believes it is important that retail health care companies' Terms of Use do not require data sharing for uses not directly related to patients' medical care in order to receive care – unless required by law (e.g., reporting of infectious diseases). Operationally, this means that the Terms of Use should be distinct from the Notice of Privacy Practices, with clear indication that patients are not required to sign the latter in order to receive care. Retail health care companies should provide education on this concept to reduce patient vulnerability and achieve meaningful consent.

There are four types of consent: express consent, implied consent, opt-in consent and opt-out consent. Several retail health care companies utilize opt-out consent, which assumes user consent unless they act to withdraw it. Opt-out consent requires users to take action to indicate non-consent, placing the responsibility on users to actively protect their data. When opt-out consent is coupled with deceptive wording, it may lead patients to agree to something without meaningful consent. Meaningful consent requires a patient to be given sufficient and understandable knowledge to make a valid decision. Requiring retail health care companies to use a default opt-in consent plus plain language is essential toward protecting patients' privacy and fostering health literacy. Once consent is given, it then becomes important to provide clear direction on how patients can withdraw consent. Section 1798.105(a) of the California Consumer Privacy Act grants consumers the right to request that a business delete any personal information about the consumer which the business has collected from the consumer. While the CCPA "right to be forgotten" has many exceptions that allow businesses to keep personal information, it could serve as a prototype for regulations in the retail health care arena.

RELEVANT AMA POLICY, ADVOCACY, & RESOURCES

The AMA Privacy Principles, derived primarily from AMA House of Delegates policy, serve as the foundation for AMA advocacy on privacy extrinsic to HIPAA covered entities. In addition to shifting the responsibility for privacy from individuals to data holders, the principles implore that

individuals have the right to know whether their data will be used to develop and/or train AI algorithms and hold entities accountable toward making their de-identification processes and techniques publicly available. These Principles were developed based on an identified need to extend AMA advocacy efforts beyond protections for HIPAA covered entities to (1) provide individuals with rights and protections from discrimination; (2) shift the responsibility for privacy from individuals to data holders other than HIPAA covered entities; and (3) create principles for robust enforcement, individual rights, equity, applicability, and entity responsibility. The AMA Privacy Principles advocate for the expansion of FTC oversight to consumer data that is accessed, used, or exchanged by technology companies and vendors not classified as covered entities under HIPAA. The Principles contend that "health care data" is a subjective term and one that should be evaluated by a federal agency with broad expertise in data privacy. Accordingly, the AMA Privacy Principles' use of the term "data" includes information that can be used to identify an individual, even if it is not descriptive on its face, such as IP addresses and advertising identifiers from mobile phones.

While the AMA Privacy Principles recognize a role for the FTC, it is important to note why the OCR is absent from the discussion. The OCR administers and enforces HIPAA regulations with a focus on PHI, and, therefore, expanding OCR's HIPAA legislative umbrella to include technology companies and vendors not classified as covered entities was a consideration. However, it was recognized that (1) OCR lacks the structure, resources, and expertise to regulate technology companies and vendors, who are themselves new entrants into the health care arena, and (2) an existing federal agency is better equipped to regulate health data that flows outside the traditional HIPAA covered entity arena. Furthermore, extending HIPAA protections for PHI to non-HIPAA covered technology companies and vendors could create a gap in needed privacy policies.

Although the Office of the National Coordinator for Health Information Technology (ONC) is not mentioned in the AMA Privacy Principles, it has a role in ensuring that sensitive medical information regarding reproductive health, sexual orientation, gender identity, and substance use disorder is placed behind a firewall in the electronic health record as well as when it is requested and shared with others using national health information exchanges, such as under ONC's Trusted Exchange Framework and Common Agreement. The 21st Century Cures Act lifted limitations on the scope of ePHI, allowing information blocking regulations to go into full effect. Physicians who interfere with the access, exchange, or use of ePHI could be considered "information blockers" and subject to financial penalties, making it difficult for them to protect sensitive information.

The AMA's longstanding goal to support strong protections for patient privacy is reinforced by several policies, including those that:

- Advocate for legislation that aligns mobile health apps and other digital health tools with the AMA Privacy Principles (Policy D-315.968);
- Oppose the sale or transfer of medical history data and contact information for use in marketing or advertising (Policy D-315.973);
- Engage with stakeholders to identify relevant guiding principles to promote a vibrant, useful, and trustworthy mHealth market (Policy D-480.972);
- Advocate for narrowing the definition of "health care operations" to include only those activities that are routine and critical for general business operations and that cannot be reasonably undertaken with de-identified health information (Policy H-315.975);
- Support strong protections for patient privacy and, in general, require that patient medical records be kept strictly confidential unless waived by the patient in a meaningful way, de-

identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of patient privacy or breaches of confidentiality (Policy H-315.983);

- Work to ensure that computer-based patient record systems and networks, and the legislation and regulations governing their use, include adequate technical and legal safeguards for protecting the confidentiality, integrity, and security of patient data (Policy H-315.989); and
- Support that mHealth apps and associated devices, trackers and sensors must abide by applicable laws addressing the privacy and security of patients' medical information (Policy
- H-480.943).

AMA policy has been developed related to the potential complications introduced by the intersection of AI and patient privacy, including those that:

- Re-examine existing guidance relevant to the confidentiality of patient information, striving to preserve the benefits of widespread use of de-identified patient data for purposes of promoting quality improvement, research, and public health while mitigating the risks of re-identification of such data (Policy D-315.969);
- Support efforts to promote transparency in the use of de-identified patient data and to protect patient privacy by developing methods of, and technologies for, de-identification of patient information that reduce the risk of re-identification of such data (Policy H-315.962); and
- Promote development of thoughtfully designed, high-quality, clinically validated health care AI that safeguards patients' privacy interests and preserves the security and integrity of personal information (Policy H-480.940).

The AMA has written several comment letters addressing the issue of patient privacy, including a December 2018 letter to NIST which references the tenets of Policy H-315.983, noting that when breaches of confidentiality are compelled by concerns for public health and safety, those breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest possible to achieve the necessary end. In a February 2019 letter to the Office for Civil Rights, the AMA offers suggestions on a Request for Information about modifying HIPAA Rules to improve coordinated care, including how the regulations can be revised to promote the goals of value-based care and care coordination while preserving and protecting the privacy and security of a patient's health information. In May 2019, the AMA submitted patient privacy comments to several recipients, including the Office of the National Coordinator for Health Information Technology and the Centers for Medicare & Medicaid Services, and the FTC. While slightly different audiences, the message for each was similar, with a focus on the AMA approach to privacy. The AMA outlined how data segmentation is critical for health information exchange, regardless of where the data resides, how it is used, or with whom it is exchanged. Consistent with that approach, patient consent and privacy, data provenance, governance, and state and federal law compliance must be inherent in the development of technology. A June 2023 letter to the National Governors Association urged that comprehensive state legislative privacy proposals provide adequate protections for consumer health data, especially health data obtained by apps and other devices or organizations that do not fall within HIPAA or state privacy laws. In August 2023, the AMA submitted written comments to the FTC regarding the Health Breach Notification Rule, noting the deficiencies in regulation of health apps. A September 2023 AMA letter to Senator Bill Cassidy in response to his request for information outlines the distinction between PHI and health information outside of HIPAA, and the potential for harm to individuals caused by confusion between the two.

In addition to advocacy, the AMA provides members with robust resources on the issue of patient privacy. The AMA health data privacy framework surveyed patient perspectives to shed light on

fundamental data privacy issues that can impact individuals nationwide, while the AMA patient privacy webpage provides resources to ensure that patients have meaningful controls over their PHI. As part of the AMA Patient Access Playbook, the AMA has developed a case for privacy by design in app development. The 2023 AMA Principles for Augmented Intelligence Development, Deployment, and Use address privacy and cybersecurity as well as establish guardrails around payer use of AI in automated denials.

DISCUSSION

While HIPAA was enacted in 1996, misconceptions have muddied the waters around what is and is not a covered entity or business associate, and what is or is not PHI. Given that HIPAA only governs covered entities and business associates, concerns arise in the regulation of entities currently beyond the scope of HIPAA, such as digital health platforms, apps, and other similar software programs that collect, use, store, and share personal health data. Under federal law there is no floor – no minimum threshold – for an organization's privacy policy other than it cannot be unfair or deceptive. Thus, any health app or digital health platform can word their stated privacy policy in a weak, evasive, easy-to-comply-with manner that will sound reassuring to the consumers who choose to read it. Furthermore, there is confusion surrounding retail health care companies' HIPAA status, as they require patients to read and comprehend several documents together in order to understand their rights. Determining which organizations HIPAA applies to can be difficult for the layperson.

The Council therefore recommends a series of principles to address retail health care companies' handling of PHI. Any health care providing entity, or one that is facilitating the referral of patients for care, regardless of whether it provides the care directly, must be held to the standard of a HIPAA covered entity, complete with a privacy wall between the health and non-health lines of business to eliminate sharing of PHI for uses not directly related to patients' medical care. Retail health care companies should be prohibited from utilizing "clickwrap" agreements, which permit patients to use a service without affirmatively consenting to the data sharing. It is also important that retail health care companies' Terms of Use do not require data sharing for uses not directly related to patients' medical care in order to receive care unless required by law. Operationally, this means that the Terms of Use should be distinct from the Notice of Privacy Practices, with clear indication that patients are not required to sign the latter in order to receive care. Requiring retail health care companies to use a default opt-in consent plus plain language is essential toward protecting patients' privacy and fostering health literacy. Opt-in user consent requires patients to acknowledge the proposed data activity, understand the purposes for collection, and agree to have their data collected, processed, and stored. Once consent is given, it then becomes important to provide clear direction on how patients can withdraw consent.

The Council also recommends reaffirmation of policies that advocate for legislation that aligns mobile health apps and other digital health tools with the AMA Privacy Principles, supports efforts to promote transparency in the use of de-identified patient data, and promotes development of thoughtfully designed, high-quality, clinically validated health care AI that safeguards patients' privacy interests and preserves the security and integrity of personal information.

RECOMMENDATIONS

The Council on Medical Service recommends that the following be adopted, and the remainder of the report be filed:

1. That our American Medical Association (AMA) will:
   (a) support regulatory guidance to establish a privacy wall between the health business and non-health business of retail health care companies to eliminate sharing of protected health information, re-identifiable patient data, or data that could be reasonably be used to re-identify a patient when combined with other data for uses not directly related to patients' medical care;
   (b) support the prohibition of Terms of Use that require data sharing for uses not directly related to patients' medical care in order to receive care, while still allowing data sharing where required by law (e.g., infectious disease reporting);
   (c) support the separation of consents required to receive care from any consents to share data for non-medical care reasons, with clear indication that patients do not need to sign the data-sharing agreements in order to receive care;
   (d) support the prohibition of "clickwrap" contracts for use of a health care service without affirmative patient consent to data sharing;
   (e) support the requirement that retail health care companies must use an active opt-in selection for obtaining meaningful consent for data use and disclosure, otherwise the default should be that the patient does not consent to disclosure;
   (f) support the requirement that retail health care companies clearly indicate how patients can withdraw consent and request deletion of data retained by the non-health care providing units, which should be by a means no more onerous than providing the initial consent. (New HOD Policy)

2. That our AMA reaffirm Policy D-315.968, which advocates for legislation that aligns mobile health apps and other digital health tools with the AMA Privacy Principles. (Reaffirm HOD Policy)

3. That our AMA reaffirm Policy H-315.962, which supports efforts to promote transparency in the use of de-identified patient data and to protect patient privacy by developing methods of, and technologies for, de-identification of patient information that reduce the risk of re-identification of such data. (Reaffirm HOD Policy)

4. That our AMA reaffirm Policy H-480.940, which promotes development of thoughtfully designed, high-quality, clinically validated health care AI that safeguards patients' privacy interests and preserves the security and integrity of personal information. (Reaffirm HOD Policy)

5. Rescind Policy H-315.960, as having been completed with this report. (Rescind HOD Policy)

Fiscal Note: Less than $500.

REFERENCES

[1] Lagasse, J, Healthcare Finance, "Retail Clinics Seeing Utilization Soar, Popularity Grow," June 2023. Available at: https://www.healthcarefinancenews.com/news/retail-clinics-seeing-utilization-soar-popularity-grow#:~:text=In%202023%2C%20there%20were%20more,account%20for%2062%25%20of %20locations
[2] FAIR Health White Paper, FH Healthcare Indicators and FH Medical Price Index, March 26, 2024. Available at: https://s3.amazonaws.com/media2.fairhealth.org/whitepaper/asset/FH%20Healthcare%20Indicators%20and%20FH%20Medical%20Price%20Index%202024%20-%20A%20FAIR %Health%20White%20Paper.pdf
[3] Definitive Healthcare, "How Many Retail Clinics Are in the U.S.?" April 2023. Available at: https://www.definitivehc.com/resources/healthcare-insights/retail-clinics-us#:~:text=There%20were %201%2C801%20active%20retail,states%20as%20of%20March%202023
[4] Baxter, A, HealthExec, "Patient Privacy Concerns Are Rising," July 2022. Available at: https://healthexec.com/topics/health-it/cybersecurity/patient-privacy-concerns-are-rising
[5] Reed, T, Axios, "Amazon Launches Drug Delivery By Drone," October 2023. Available at: https://www.axios.com/2023/10/18/amazon-drone-drug-delivery-texas?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosvitals&stream=top
[6] Hales, M, The HIPAA E-Tool, "Amazon Clinic Raises HIPAA Questions," May 2023. Available at: https://thehipaaetool.com/amazon-clinic-raises-hipaa-questions/#:~:text=Amazon's%20privacy %20page %20explains%20that, a%20HIPAA%20%E2%80%9Cbusiness%20associate%E2%80%9C
[7] Adler, S, The HIPAA Journal, "Senators Demand Answers on Amazon Clinic's Uses of Customer Data," June 2023. Available at: https://www.hipaajournal.com/senators-demand-answers-on-amazon-clinics-uses-of-customer-data/
[8] Leonard, B, et al., Politico, "Amazon Called to Account – on Health Data," June 2023. Available at: https://www.politico.com/newsletters/future-pulse/2023/06/16/amazon-called-to-account-on-health-data-00102301
[9] Markus, P, Healthcare IT News, "How far will FTC expand Health Breach Notification Rule enforcement?" December 2023. Available at: https://www.healthcareitnews.com/blog/how-far-will-ftc-expand-health-breach-notification-rule-enforcement
[10] Olivero, A, et al., International Association of Privacy Professionals, "Washington's MyHealth, MyData Act," April 2023. Available at: https://iapp.org/resources/article/washington-my-health-my-data-act-overview/
[11] Greene, A, Davis Wright Tremaine LLP Privacy & Security Law, "How State General Privacy Laws Apply to Healthcare Providers," January 2023. Available at: https://www.dwt.com/blogs/privacy--security-law-blog/2023/01/privacy-healthcare-providers-hipaa
[12] McKeon, J, Health IT Security, "FTC Warns Amazon About Improper Health Data Sharing Following One Medical," March 2023. Available at: https://healthitsecurity.com/news/ftc-warns-amazon-about-improper-health-data-sharing-following-one-medical-acquisition
[13] Alder, S, The HIPAA Journal, "Senators Demand Answers on Amazon Clinic's Uses of Customer Data," June 2023. Available at: https://www.hipaajournal.com/senators-demand-answers-on-amazon-clinics-uses-of-customer-data/
[14] Seh AH, Zarour M, Alenezi M, Sarkar AK, Agrawal A, Kumar R, Khan RA. Healthcare Data Breaches: Insights and Implications. Healthcare (Basel). 2020 May 13;8(2):133. doi: 10.3390/healthcare8020133. PMID: 32414183; PMCID: PMC7349636.
[15] Cornell Law School, Legal Information Institute, "45 CFR § 164.514 - Other requirements relating to uses and disclosures of protected health information." Available at: https://www.law.cornell.edu/cfr/text/45/164.514#:~:text=(a) percent20Standard percent3A percent20De percent2D,not percent20individually percent20identifiable percent20health percent20information
[16] Alder, S, The HIPAA Journal, "HIPAA, Healthcare Data, and Artificial Intelligence," December 2022. Available at: https://www.hipaajournal.com/hipaa-healthcare-data-and-artificial-intelligence/

Council on Medical Service Report 7-A-24
Ensuring Privacy in Retail Health Care Settings
Policy Appendix

Supporting Improvements to Patient Data Privacy D-315.968
Our AMA will (1) strengthen patient and physician data privacy protections by advocating for legislation that reflects the AMA's Privacy Principles with particular focus on mobile health apps and other digital health tools, in addition to non-health apps and software capable of generating patient data and (2) will work with appropriate stakeholders to oppose using any personally identifiable data to identify patients, potential patients who have yet to seek care, physicians, and any other health care providers who are providing or receiving health care that may be criminalized in a given jurisdiction.
Res. 227, A-22 Modified: Res. 230, I-22 Reaffirmation: A-23

Research Handling of De-Identified Patient Information D-315.969
The Council on Ethical and Judicial Affairs will consider re-examining existing guidance relevant to the confidentiality of patient information, striving to preserve the benefits of widespread use of de-identified patient data for purposes of promoting quality improvement, research, and public health while mitigating the risks of re-identification of such data.
BOT Rep. 16, I-21

Preventing Inappropriate Use of Patient Protected Medical Information in the Vaccination Process D-315.973
Our AMA will: (1) advocate to prohibit the use of patient/customer information collected by retail pharmacies for COVID-19 vaccination scheduling and/or the vaccine administration process for commercial marketing or future patient recruiting purposes, especially any targeting based on medical history or conditions; and (2) oppose the sale or transfer of medical history data and contact information accumulated through the scheduling or provision of government-funded vaccinations to third parties for use in marketing or advertising.
Res. 232, A-21

Guidelines for Mobile Medical Applications and Devices D-480.972
1. Our AMA will monitor market developments in mobile health (mHealth), including the development and uptake of mHealth apps, in order to identify developing consensus that provides opportunities for AMA involvement.
2. Our AMA will continue to engage with stakeholders to identify relevant guiding principles to promote a vibrant, useful and trustworthy mHealth market.
3. Our AMA will make an effort to educate physicians on mHealth apps that can be used to facilitate patient communication, advice, and clinical decision support, as well as resources that can assist physicians in becoming familiar with mHealth apps that are clinically useful and evidence based.
4. Our AMA will develop and publicly disseminate a list of best practices guiding the development and use of mobile medical applications.
5. Our AMA encourages further research integrating mobile devices into clinical care, particularly to address challenges of reducing work burden while maintaining clinical autonomy for residents and fellows.
6. Our AMA will collaborate with the Liaison Committee on Medical Education and Accreditation Council for Graduate Medical Education to develop germane policies, especially with

consideration of potential financial burden and personal privacy of trainees, to ensure more uniform regulation for use of mobile devices in medical education and clinical training.
7. Our AMA encourages medical schools and residency programs to educate all trainees on proper hygiene and professional guidelines for using personal mobile devices in clinical environments.
8. Our AMA encourages the development of mobile health applications that employ linguistically appropriate and culturally informed health content tailored to linguistically and/or culturally diverse backgrounds, with emphasis on underserved and low-income populations.
CSAPH Rep. 5, A-14 Appended: Res. 201, A-15 Appended: Res. 305, I-16 Modified: Res. 903, I-19

Research Handling of De-Identified Patient Information H-315.962
Our AMA supports efforts to promote transparency in the use of de-identified patient data and to protect patient privacy by developing methods of, and technologies for, de-identification of patient information that reduce the risk of re-identification of such information.
BOT Rep. 16, I-21 Reaffirmation: A-22

Police, Payer, and Government Access to Patient Health Information H-315.975
(1) Our AMA advocates vigorously, with respect to the final privacy rule or other privacy legislation, to define "health care operations" narrowly to include only those activities and functions that are routine and critical for general business operations and that cannot reasonably be undertaken with de-identified information.
(2) Our AMA advocates vigorously, with respect to the final privacy rule or other privacy legislation, that the Centers for Medicare & Medicaid Services (CMS) and other payers shall have access to medical records and individually identifiable health information solely for billing and payment purposes, and routine and critical health care operations that cannot reasonably be undertaken with de-identified health information.
(3) Our AMA advocates vigorously, with respect to the final privacy rule or other privacy legislation, that CMS and other payers may access and use medical records and individually identifiable health information for non-billing, non-payment purposes and non-routine, non-critical health care operations that cannot reasonably be undertaken with de-identified health information, only with the express written consent of the patient or the patient's authorized representative, each and every time, separate and apart from blanket consent at time of enrollment.
(4) Our AMA advocates vigorously, with respect to the final privacy rule or other privacy legislation that no government agency, including law enforcement agencies, be permitted access to medical records or individually identifiable health information (except for any discretionary or mandatory disclosures made by physicians and other health care providers pursuant to ethical guidelines or to comply with applicable state or federal reporting laws) without the express written consent of the patient, or a court order or warrant permitting such access.
(5) Our AMA continues to strongly support and advocate a minimum necessary standard of disclosure of individually identifiable health information requested by payers, so that the information necessary to accomplish the intended purpose of the request be determined by physicians and other health care providers, as permitted under the final privacy rule.
Res. 246, A-01 Reaffirmation I-01 Reaffirmation A-02 Reaffirmed: BOT Rep. 19, I-06 Reaffirmation A-07 Reaffirmed: BOT Rep. 19, A-07 Reaffirmed: BOT Rep. 22, A-17 Reaffirmed: BOT Rep. 16, I-21

Patient Privacy and Confidentiality H-315.983
1. Our AMA affirms the following key principles that should be consistently implemented to evaluate any proposal regarding patient privacy and the confidentiality of medical information: (a)

That there exists a basic right of patients to privacy of their medical information and records, and that this right should be explicitly acknowledged; (b) That patients' privacy should be honored unless waived by the patient in a meaningful way or in rare instances when strong countervailing interests in public health or safety justify invasions of patient privacy or breaches of confidentiality, and then only when such invasions or breaches are subject to stringent safeguards enforced by appropriate standards of accountability; (c) That patients' privacy should be honored in the context of gathering and disclosing information for clinical research and quality improvement activities, and that any necessary departures from the preferred practices of obtaining patients' informed consent and of de-identifying all data be strictly controlled; (d) That any information disclosed should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of disclosure; and (e) That the Health Insurance Portability and Accountability Act of 1996 (HIPAA) be the minimal standard for protecting clinician-patient privilege, regardless of where care is received.

2. Our AMA affirms: (a) that physicians and medical students who are patients are entitled to the same right to privacy and confidentiality of personal medical information and medical records as other patients, (b) that when patients exercise their right to keep their personal medical histories confidential, such action should not be regarded as fraudulent or inappropriate concealment, and (c) that physicians and medical students should not be required to report any aspects of their patients' medical history to governmental agencies or other entities, beyond that which would be required by law.

3. Employers and insurers should be barred from unconsented access to identifiable medical information lest knowledge of sensitive facts form the basis of adverse decisions against individuals. (a) Release forms that authorize access should be explicit about to whom access is being granted and for what purpose and should be as narrowly tailored as possible. (b) Patients, physicians, and medical students should be educated about the consequences of signing overly-broad consent forms. (c) Employers and insurers should adopt explicit and public policies to assure the security and confidentiality of patients' medical information. (d) A patient's ability to join or a physician's participation in an insurance plan should not be contingent on signing a broad and indefinite consent for release and disclosure.

4. Whenever possible, medical records should be de-identified for purposes of use in connection with utilization review, panel credentialing, quality assurance, and peer review.

5. The fundamental values and duties that guide the safekeeping of medical information should remain constant in this era of computerization. Whether they are in computerized or paper form, it is critical that medical information be accurate, secure, and free from unauthorized access and improper use.

6. Our AMA recommends that the confidentiality of data collected by race and ethnicity as part of the medical record, be maintained.

7. Genetic information should be kept confidential and should not be disclosed to third parties without the explicit informed consent of the tested individual.

8. When breaches of confidentiality are compelled by concerns for public health and safety, those breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest possible to achieve the necessary end.

9. Law enforcement agencies requesting private medical information should be given access to such information only through a court order. This court order for disclosure should be granted only if the law enforcement entity has shown, by clear and convincing evidence, that the information sought is necessary to a legitimate law enforcement inquiry; that the needs of the law enforcement authority cannot be satisfied by non-identifiable health information or by any other information; and that the law enforcement need for the information outweighs the privacy interest of the

individual to whom the information pertains. These records should be subject to stringent security measures.
10. Our AMA must guard against the imposition of unduly restrictive barriers to patient records that would impede or prevent access to data needed for medical or public health research or quality improvement and accreditation activities. Whenever possible, de-identified data should be used for these purposes. In those contexts where personal identification is essential for the collation of data, review of identifiable data should not take place without an institutional review board (IRB) approved justification for the retention of identifiers and the consent of the patient. In those cases where obtaining patient consent for disclosure is impracticable, our AMA endorses the oversight and accountability provided by an IRB.
11. Marketing and commercial uses of identifiable patients' medical information 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 first give their uncoerced permission after being fully informed about the purpose of such disclosures
12. Our AMA, in collaboration with other professional organizations, patient advocacy groups and the public health community, should continue its advocacy for privacy and confidentiality regulations, including: (a) The establishment of rules allocating liability for disclosure of identifiable patient medical information between physicians and the health plans of which they are a part, and securing appropriate physicians' control over the disposition of information from their patients' medical records. (b) The establishment of rules to prevent disclosure of identifiable patient medical information for commercial and marketing purposes; and (c) The establishment of penalties for negligent or deliberate breach of confidentiality or violation of patient privacy rights.
13. Our AMA will pursue an aggressive agenda to educate patients, the public, physicians and policymakers at all levels of government about concerns and complexities of patient privacy and confidentiality in the variety of contexts mentioned.
14. Disclosure of personally identifiable patient information to public health physicians and departments is appropriate for the purpose of addressing public health emergencies or to comply with laws regarding public health reporting for the purpose of disease surveillance.
15. In the event of the sale or discontinuation of a medical practice, patients should be notified whenever possible and asked for authorization to transfer the medical record to a new physician or care provider. Only de-identified and/or aggregate data should be used for "business decisions," including sales, mergers, and similar business transactions when ownership or control of medical records changes hands.
16. The most appropriate jurisdiction for considering physician breaches of patient confidentiality is the relevant state medical practice act. Knowing and intentional breaches of patient confidentiality, particularly under false pretenses, for malicious harm, or for monetary gain, represents a violation of the professional practice of medicine.
17. Our AMA Board of Trustees will actively monitor and support legislation at the federal level that will afford patients protection against discrimination on the basis of genetic testing.
18. Our AMA supports privacy standards that would require pharmacies to obtain a prior written and signed consent from patients to use their personal data for marketing purposes.
19. Our AMA supports privacy standards that require pharmacies and drug store chains to disclose the source of financial support for drug mailings or phone calls.
20. Our AMA supports privacy standards that would prohibit pharmacies from using prescription refill reminders or disease management programs as an opportunity for marketing purposes.
21. Our AMA will draft model state legislation requiring consent of all parties to the recording of a physician-patient conversation.

BOT Rep. 9, A-98 Reaffirmation I-98 Appended: Res. 4, and Reaffirmed: BOT Rep. 36, A-99 Appended: BOT Rep. 16 and Reaffirmed: CSA Rep. 13, I-99 Reaffirmation A-00 Reaffirmed: Res. 246 and 504 and Appended Res. 504 and 509, A-01 Reaffirmed: BOT Rep. 19, I-01 Appended: Res. 524, A-02 Reaffirmed: Sub. Res. 206, A-04 Reaffirmed: BOT Rep. 24, I-04 Reaffirmed: BOT Rep. 19, I-06 Reaffirmation A-07 Reaffirmed: BOT Rep. 19, A-07 Reaffirmed: CEJA Rep. 6, A-11 Reaffirmed in lieu of Res. 705, A-12 Reaffirmed: BOT Rep. 17, A-13 Modified: Res. 2, I-14 Reaffirmation: A-17 Modified: BOT Rep. 16, A-18 Appended: Res. 232, A-18 Reaffirmation: I-18 Reaffirmed: Res. 219, A-21 Reaffirmed: Res. 229, A-21 Reaffirmed: BOT Rep. 12, I-21 Reaffirmed: BOT Rep. 22, A-22 Reaffirmation: A-23

Confidentiality of Computerized Patient Records H-315.989
The AMA will continue its leadership in protecting the confidentiality, integrity, and security of patient-specific data; and will continue working to ensure that computer-based patient record systems and networks, and the legislation and regulations governing their use, include adequate technical and legal safeguards for protecting the confidentiality, integrity, and security of patient data.
BOT Rep. F, A-93 Reaffirmation I-99 Reaffirmed: BOT Rep. 19, I-06 Reaffirmed: BOT Rep. 19, A-07 Reaffirmed in lieu of Res. 818, I-07 Reaffirmation I-08 Reaffirmation A-10 Reaffirmed: BOT Rep. 17, A-13

Augmented Intelligence in Health Care H-480.940
As a leader in American medicine, our AMA has a unique opportunity to ensure that the evolution of augmented intelligence (AI) in medicine benefits patients, physicians, and the health care community.
To that end our AMA will seek to:
1. Leverage its ongoing engagement in digital health and other priority areas for improving patient outcomes and physicians' professional satisfaction to help set priorities for health care AI.
2. Identify opportunities to integrate the perspective of practicing physicians into the development, design, validation, and implementation of health care AI.
3. Promote development of thoughtfully designed, high-quality, clinically validated health care AI that:
a. is designed and evaluated in keeping with best practices in user-centered design, particularly for physicians and other members of the health care team;
b. is transparent;
c. conforms to leading standards for reproducibility;
d. identifies and takes steps to address bias and avoids introducing or exacerbating health care disparities including when testing or deploying new AI tools on vulnerable populations; and
e. safeguards patients and other individuals privacy interests and preserves the security and integrity of personal information.
4. Encourage education for patients, physicians, medical students, other health care professionals, and health administrators to promote greater understanding of the promise and limitations of health care AI.
5. Explore the legal implications of health care AI, such as issues of liability or intellectual property, and advocate for appropriate professional and governmental oversight for safe, effective, and equitable use of and access to health care AI.
BOT Rep. 41, A-18

Integration of Mobile Health Applications and Devices into Practice H-480.943
1. Our AMA supports the establishment of coverage, payment and financial incentive mechanisms to support the use of mobile health applications (mHealth apps) and associated devices, trackers and sensors by patients, physicians and other providers that: (a) support the establishment or continuation of a valid patient-physician relationship; (b) have a high-quality clinical evidence base to support their use in order to ensure mHealth app safety and effectiveness; (c) follow evidence-based practice guidelines, especially those developed and produced by national medical specialty societies and based on systematic reviews, to ensure patient safety, quality of care and positive health outcomes; (d) support care delivery that is patient-centered, promotes care coordination and facilitates team-based communication; (e) support data portability and interoperability in order to promote care coordination through medical home and accountable care models; (f) abide by state licensure laws and state medical practice laws and requirements in the state in which the patient receives services facilitated by the app; (g) require that physicians and other health practitioners delivering services through the app be licensed in the state where the patient receives services, or be providing these services as otherwise authorized by that state's medical board; and (h) ensure that the delivery of any services via the app be consistent with state scope of practice laws.
2. Our AMA supports that mHealth apps and associated devices, trackers and sensors must abide by applicable laws addressing the privacy and security of patients' medical information.
3. Our AMA encourages the mobile app industry and other relevant stakeholders to conduct industry-wide outreach and provide necessary educational materials to patients to promote increased awareness of the varying levels of privacy and security of their information and data afforded by mHealth apps, and how their information and data can potentially be collected and used.
4. Our AMA encourages the mHealth app community to work with the AMA, national medical specialty societies, and other interested physician groups to develop app transparency principles, including the provision of a standard privacy notice to patients if apps collect, store and/or transmit protected health information.
5. Our AMA encourages physicians to consult with qualified legal counsel if unsure of whether an mHealth app meets Health Insurance Portability and Accountability Act standards and also inquire about any applicable state privacy and security laws.
6. Our AMA encourages physicians to alert patients to the potential privacy and security risks of any mHealth apps that he or she prescribes or recommends, and document the patient's understanding of such risks
7. Our AMA supports further development of research and evidence regarding the impact that mHealth apps have on quality, costs, patient safety and patient privacy.
8. Our AMA encourages national medical specialty societies to develop guidelines for the integration of mHealth apps and associated devices into care delivery.
CMS Rep. 06, I-16 Reaffirmation: A-17 Reaffirmation: A-23