At the 2017 Annual Meeting the House of Delegates adopted Policy D-315.976, “Ownership of Patient Data,” which asks that our American Medical Association undertake a study on the misuse of patient information by hospitals, corporations, insurance companies, and big pharma, including the impact on patient safety, quality of care, and access to care when a patient’s data is withheld from his or her physician.

The testimony on this resolution was unanimously in favor of adoption. Those who spoke discussed the many challenges related to accessing patient data and medical records by physicians, and agreed that a study is needed to better identify these obstacles and begin exploring solutions to the use and misuse of patient information.

This informational report provides an overview of the current laws and regulations at the state and federal levels that address ownership, access and use of patient data including under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its implementing regulations. It also looks at controls and processes in place to address physician and healthcare industry access and use of patient information.

LEGAL AND REGULATORY OVERVIEW

Ownership of, and access to, patient data contained in a medical record are distinct concepts under the law. State laws vary on the topic of who owns a patient’s medical record. As depicted in the following graphic from Health Information & the Law1 the majority of state legislatures either grant ownership of the medical record to the clinician or institution, or remain silent on medical
Ownership of patient data is not specified under HIPAA. Patients, however, have broad access rights to their protected health information (PHI). Patients can also exercise control over whether and how their health information is used and disclosed for certain purposes, including marketing. The following points are highlighted for patients by the U.S. Department of Health & Human Services Office of Civil Rights document titled “Your Health Information Privacy Rights”:

1. Generally, patient health information cannot be used for purposes not directly related to care without permission. For example, a doctor cannot give it to a patient’s employer, or share it for things like marketing and advertising, without written patient authorization.
2. Patients can ask that their health information not be shared with certain people, groups, or companies.

The Office for Civil Rights (OCR) has an online complaint portal in which anyone can file a complaint against covered entities and their business associates if there is a potential violation of an individual’s health information privacy rights or other violation of the Privacy, Security, or Breach Notification Rules. A “Covered Entity” is defined as either a health plan, health care clearinghouse, or health care provider who transmits PHI in electronic form. “Business Associate” is defined in part as a person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI. Additionally, a Business Associate may also be a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. If OCR determines that a covered entity or business associate may have violated the HIPAA Rules, that entity or business associate must either voluntarily comply with the HIPAA Rules, take corrective action, or agree to a settlement with the injured party. Additionally, a civil monetary penalty (CMP) may be imposed on the covered entity if the corrective action is not viewed as satisfactory.

PHYSICIAN ACCESS TO PATIENT RECORDS

Much of the discussion on this resolution centered on the obstacles in accessing patient and medical record data by physicians. This can be a symptom of the physician’s contract with the hospital or healthcare entity they are employed by or contracted for services with, or the electronic healthcare record vendor that they or their employer has contracted with.

Contractual Considerations – Employment Agreements

In cases where a physician is an employee of a hospital or other healthcare entity, access to patient and medical record data both during and following employment is often addressed by the employment agreement. The AMA, as well as many state medical societies, provides physicians resources to assist in navigating various issues and ensuring a fair and comprehensive employment agreement. This is especially important during separation.

Depending on its terms, an employment or independent contractor (IC) arrangement between a physician and a hospital or health system should specify who owns the patient records and patient data, and which parties have access rights to the data, including after termination. The parties will negotiate their rights with respect to ownership of and access to the records for specified purposes, including upon patient request.

The “AMA Annotated Model Physician-Hospital Employment Agreement” addresses access to patient records and confidentiality in Section 8.7. While continuity of care is a high priority upon the termination of the contractual employment relationship between a hospital and a physician,
equally important is contractual language that acknowledges the physician’s entitlement to copies of patient charts and records. “The employer may wish to specify that, upon termination, the physician will not be entitled to keep or copy charts, files, or patient lists;” however, it is common practice to negotiate a provision that allows the physician to obtain the patient records after termination for situations such as a malpractice action, administrative investigation or proceeding against the physician, as they would be necessary to the physician’s defense.

**AMA Advocacy Efforts and Resources**

The AMA model state bill titled “Physician Employment Patient Notification and Records Act” states that, in order to ensure that the termination of their physicians’ employment does not disrupt their care; patients must be timely provided with information enabling them to obtain care from alternative physicians or continue to receive care from their physicians post-termination. The model bill also states that access to medical records should be addressed in the employment agreement and should state that the physician is entitled to copies of patient charts and records relating to the physician’s provision of physician services: (1) upon written request from the patient, or (2) when records are necessary to address any current or future legal, professional, administrative, regulatory, or other issues, claims, allegations, proceedings, or investigations against, involving or in connection with those services.

The AMA Advocacy Resource Center (ARC) has developed a legislative campaign with the goal of assisting physicians with issues throughout the employment spectrum including negotiating employment contracts, maintaining autonomy during employment, and terminating the relationship.

**Federal Regulation and Guidance**

The U.S. Department of Health and Human Services (HHS) has also weighed in on the related matter of charging for access to patient or medical records. In March of 2016, OCR issued new guidance including the stipulation that in the case of a request for an electronic copy of PHI maintained electronically, covered entities may charge a flat fee not to exceed $6.50 (inclusive of all labor, supplies, and postage).

**Accessing Data through an Electronic Health Record (EHR) Vendor**

The second party with which a physician can encounter issues regarding access to patient and medical record data is with their electronic health records vendor. Concerns over ensuring data are readily available to physicians and patients, prompted HHS and the Office of the National Coordinator (ONC) to release a Health IT Playbook to help clinicians navigate the EHR market. HHS and ONC also have developed an EHR contracting guide, “EHR Contracts Untangled: Selecting Wisely, Negotiating Terms, and Understanding the Fine Print.” The Health IT Playbook and contracting guide are meant to assist clinicians and healthcare institutions in negotiating contract terms with EHR vendors. The publication includes guidance and sample contract terms addressing compliance with HIPAA and the control and access to EHR data - including the avoidance of data blocking.

**Contractual Considerations – EHR Vendor Agreement**

The use of an EHR contract, including a Business Associate Agreement (BAA), can provide a covered entity, such as a physician, the legal protection necessary to use and disclose patient PHI with a health information exchange (HIE) or third party subcontractor for various purposes. These
activities may include health care activities, including but not limited to, claims processing, data analysis, or quality assurance.

Physicians are encouraged to ensure the contract with the EHR vendor clearly defines data rights. Failing to clearly address data access rights in the BAA and any other vendor contract can severely impact the physician’s ability to share data with patient registries and HIEs as well as easily transition to a new EHR vendor in the future.

The EHR vendor contract and BAA should also clearly identify what the EHR can and cannot do with the data that is created and used by the physician. The vendor agreement or BAA should address whether or not the vendor is permitted to aggregate de-identified data across different covered entities for medical research, population health management, or other purposes.

**AMA Tools and Resources**

The AMA’s Steps Forward™ module titled “Electronic Records Software Selection and Purchase” provides guidance on negotiating favorable contract terms. The AMA also has model legislation created in response to Policy D-478.972 that required the AMA to develop model state legislation to eliminate pricing barriers to EHR interfaces and connections to HIEs. The bill, titled “An Act to Improve the Transparency of Electronic Health Record Systems Costs and Promote Data Sharing,” identifies appropriate disclosures including data sharing capabilities and detailed fees.

**Federal Regulations and Guidance**

There are cases where it may be challenging to implement this guidance in today’s environment. Because of unequal bargaining power and the fact that a hospital or health system, and not an individual physician, often contracts with an EHR vendor, it can be difficult for a physician, practice, or institution to obtain favorable contract provisions. The 21st Century Cures Act (the Act) directs the Secretary of HHS to develop a strategy to reduce EHR regulatory and administrative burdens while placing new requirements upon developers as a condition of certification and maintenance of certification. These requirements address many of the AMA’s long-standing concerns with EHRs, including prohibiting vendor data blocking; improving the usability, interoperability, and security of EHRs; and testing certified EHR technology in real-world settings.

The Act provides for penalties of up to $1.0 million per instance for any developers, networks, or exchanges that the Office of Inspector General (OIG) of HHS finds to have committed information blocking.

The AMA has actively provided feedback to ONC, OIG, and HHS on what should and should not be considered blocking and publically, through numerous comment letters, supports the operationalization of the Act’s information blocking requirements for health IT vendors. The AMA is expecting the release of the proposed rule around the implementation of the Act’s requirements in April of 2018.

**USE OF PATIENT RECORDS BY THE HEALTHCARE INDUSTRY**

A search on use of EHR records reveals instances where health systems and EHR vendors are entering data agreements to provide de-identified, anonymized data to organizations including medical device manufacturers, technology providers, health information aggregators and clinical researchers. Two recent examples include a partnership between Mercy Health System and Medtronic to share de-identified data from approximately 80,000 patients with heart failure to
focus on how patients respond to Cardiac Resynchronization Therapy (CRT). In another recent example Google partnered with academic medical centers to explore how machine learning can be used to mine EHR data for improved outcomes.

EHR vendors also use de-identified patient data gathered through use of their products in population health tools. In a less common scenario, some EHR vendors are providing de-identified, anonymized patient data to health information organizations (HIO) who in turn merge the data with other available datasets and license the combination to government agencies, academia, and businesses for a range of medical research and commercial purposes. This includes pharmaceutical manufacturers who use this information in various aspects of clinical development and commercialization. HIOs also use anonymized patient data to deliver evidenced-based insights about drug safety issues as well as the quality and cost of care.

The search on use of anonymized EHR records also revealed a number of white papers and opinions on the promise of using EHR data for clinical research and improving outcomes stating, however, that there are a number of challenges yet to be overcome to make this effective.

A LOOK FORWARD

A scan of the health technology market shows that data continues to grow in importance. Several companies have announced initiatives and platforms that provide patients access and control of their information. These organizations include a Virginia-based Health IT company, Health Wizz, who has created a patient-data platform that allows patients pull their data into the Health Wizz app via EHR patient portals and then use the DirectTrust framework to send their data to providers and other organizations. Apple is giving iPhone users a means to download their health records from a patient portal, store them safely, and share them with others. The Apple feature, Health Records, is currently in a beta release which includes integration with twelve participating hospital systems. Most recently, CMS Administrator Seema Verma announced the launch of the MyHealthEData Initiative. “MyHealthEData is a government-wide initiative that will break down the barriers that contribute to preventing patients from being able to access and control their medical records. MyHealthEData makes it clear that patients should have access and control to share their data with whomever they want, making the patient the center of our health care system. Patients need to be able to control their information and know that it’s secure and private. Having access to their medical information will help them make decisions about their care, and have a better understanding of their health.”

AMA POLICY

The AMA has several policies related to this topic (see Appendix). Policy H-315.973, “Guiding Principles for the Collection, Use and Warehousing of Electronic Medical Records and Claims Data,” which was last updated and reaffirmed in 2013, establishes principles around the use of these data that include compliance with HIPAA, requires physician consent for analysis of the data, and requires data to remain accessible to authorized users for purposes of treatment, public health, patient safety, quality improvement, medical liability defense, and research.

In addition, Policy H-315.975, “Police, Payer, and Government Access to Patient Health Information,” and Policy H-315.987. “Limiting Access to Medical Records,” look to further define who should and should not have access to this information.

Finally, Ethical Opinions E-3.2.4, “Access to Medical Records by Data Collection Companies,” E-3.2.1 “Confidentiality”, and E-3.3.2, “Confidentiality and Electronic Medical Records,” are also relevant to this discussion.
CONCLUSION

This is an issue that will become more complicated as the healthcare industry looks to further connect disparate patient information in an effort to map the patient journey and improve health outcomes. Throughout the progression it is important that patients have appropriate access to their data and physicians have the tools and controls they need to be good stewards of their patients’ information while at the same time have the ability to share information to seamlessly coordinate the best care. In support of these initiatives, the AMA has actively engaged with HHS, OIG, and ONC and has broad policy in place covering all aspects of patient record maintenance, access and control.

Physicians and healthcare institutions have the ability to control use and access to the patient data they create within an EHR through agreements with the EHR vendor and business associate agreements. Additionally all PHI contained in the EHR is protected under HIPAA.

Our AMA has taken a leadership role in ensuring appropriate use and access of these data by (1) working with ONC and HHS to encourage operational implementation of provisions in the 21st Century Cures Act to prohibit EHR vendors from blocking access to data and limiting a physician’s ability to effectively utilize their EHR system; (2) providing physicians and practices with resources on negotiating employment and independent contractor agreements to assist in clarifying ownership of and access to patient information upon termination of employment or contracting; (3) supplying physicians and practices with educational tools about favorable EHR vendor contract terms covering ownership of, access to, and use of patient information; (4) educating physicians and practices on how to file a HIPAA complaint with the OCR; and (5) providing the Federation of Medicine with model legislation that ensures appropriate handling and access to patient data.

Lastly, technologies are emerging every day that are focused on putting patient data in the patient’s hands with the capability of providing access and control to the patient with a mechanism of doing so in a systematic way.
REFERENCES

4. “Individuals’ Right under HIPAA to Access their Health Information 45 CFR § 164.524” [https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/#newlyreleasedfaqs)

APPENDIX – AMA POLICIES RELATED TO THIS REPORT

**AMA Code of Medical Ethics**

**Code of Medical Ethics Opinion E-3.2.4, “Access to Medical Records by Data Collection Companies”**

Disclosing information to third parties for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality.

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

Code of Medical Ethics Opinion E-3.3.1, “Management of Medical Records”
Physicians have an ethical obligation to manage medical records appropriately.

Medical records serve important patient interests for present health care and future needs, as well as insurance, employment, and other purposes.

In keeping with the professional responsibility to safeguard the confidentiality of patients’ personal information, physicians have an ethical obligation to manage medical records appropriately.

This obligation encompasses not only managing the records of current patients, but also retaining old records against possible future need, and providing copies or transferring records to a third party as requested by the patient or the patient’s authorized representative when the physician leaves a practice, sells his or her practice, retires, or dies.

To manage medical records responsibly, physicians (or the individual responsible for the practice’s medical records) should:

(a) Ensure that the practice or institution has and enforces clear policy prohibiting access to patients’ medical records by unauthorized staff.

(b) Use medical considerations to determine how long to keep records, retaining information that another physician seeing the patient for the first time could reasonably be expected to need or want to know unless otherwise required by law, including:
   1. Immunization records, which should be kept indefinitely
   2. Records of significant health events or conditions and interventions that could be expected to have a bearing on the patient’s future health care needs, such as records of chemotherapy

(c) Make the medical record available:
   1. As requested or authorized by the patient (or the patient’s authorized representative)
   2. To the succeeding physician or other authorized person when the physician discontinues his or her practice (whether through departure, sale of the practice, retirement, or death)
   3. As otherwise required by law
(d) Never refuse to transfer the record on request by the patient or the patient’s authorized representative, for any reason.

(e) Charge a reasonable fee (if any) for the cost of transferring the record.

(f) Appropriately store records not transferred to the patient’s current physician.

(g) Notify the patient about how to access the stored record and for how long the record will be available.

(h) Ensure that records that are to be discarded are destroyed to protect confidentiality.

Code of Medical Ethics Opinion 3.3.2, “Confidentiality and Electronic Medical Records”
Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored.

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

(a) Choose a system that conforms to acceptable industry practices and standards with respect to:
   1. Restriction of data entry and access to authorized personnel
   2. Capacity to routinely monitor/audit access to records
   3. Measures to ensure data security and integrity
   4. Policies and practices to address record retrieval, data sharing, third-party access and release of information, and disposition of records (when outdated or on termination of the service relationship) in keeping with ethics guidance

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

(c) Release patient information only in keeping with ethics guidance for confidentiality.

Code of Medical Ethics Opinion 3.2.1, “Confidentiality”
Medical records serve important patient interests for present health care and future needs, as well as insurance, employment, and other purposes.

In keeping with the professional responsibility to safeguard the confidentiality of patients’ personal information, physicians have an ethical obligation to manage medical records appropriately.

This obligation encompasses not only managing the records of current patients, but also retaining old records against possible future need, and providing copies or transferring records to a third party as requested by the patient or the patient’s authorized representative when the physician leaves a practice, sells his or her practice, retires, or dies.

To manage medical records responsibly, physicians (or the individual responsible for the practice’s medical records) should:

(a) Ensure that the practice or institution has and enforces clear policy prohibiting access to patients’ medical records by unauthorized staff.
(b) Use medical considerations to determine how long to keep records, retaining information that another physician seeing the patient for the first time could reasonably be expected to need or want to know unless otherwise required by law, including:
1. Immunization records, which should be kept indefinitely
2. Records of significant health events or conditions and interventions that could be expected to have a bearing on the patient’s future health care needs, such as records of chemotherapy

(c) Make the medical record available:
1. As requested or authorized by the patient (or the patient’s authorized representative)
2. To the succeeding physician or other authorized person when the physician discontinues his or her practice (whether through departure, sale of the practice, retirement, or death)
3. As otherwise required by law

(d) Never refuse to transfer the record on request by the patient or the patient’s authorized representative, for any reason.

(e) Charge a reasonable fee (if any) for the cost of transferring the record.

(f) Appropriately store records not transferred to the patient’s current physician.

(g) Notify the patient about how to access the stored record and for how long the record will be available.

(h) Ensure that records that are to be discarded are destroyed to protect confidentiality.

AMA Policy

H-315.973, “Guiding Principles for the Collection, Use and Warehousing of Electronic Medical Records and Claims Data”
1. It is AMA policy that any payer, clearinghouse, vendor, or other entity that collects and uses electronic medical records and claims data adhere to the following principles:
   a. Electronic medical records and claims data transmitted for any given purpose to a third party must be the minimum necessary needed to accomplish the intended purpose.
   b. All covered entities involved in the collection and use of electronic medical records and claims data must comply with the HIPAA Privacy and Security Rules.
   c. The physician must be informed and provide permission for any analysis undertaken with his/her electronic medical records and claims data, including the data being studied and how the results will be used.
   d. Any additional work required by the physician practice to collect data beyond the average data collection for the submission of transactions (e.g., claims, eligibility) must be compensated by the entity requesting the data.
   e. Criteria developed for the analysis of physician claims or medical record data must be open for review and input by relevant outside entities.
   f. Methods and criteria for analyzing the electronic medical records and claims data must be provided to the physician or an independent third party so re-analysis of the data can be performed.
   g. An appeals process must be in place for a physician to appeal, prior to public release, any adverse decision derived from an analysis of his/her electronic medical records and claims data.
   h. Clinical data collected by a data exchange network and searchable by a record locator service must be accessible only for payment and health care operations.
2. It is AMA policy that any physician, payer, clearinghouse, vendor, or other entity that warehouses electronic medical records and claims data adhere to the following principles:

   a. The warehouse vendor must take the necessary steps to ensure the confidentiality, integrity, and availability of electronic medical records and claims data while protecting against threats to the security or integrity and unauthorized uses or disclosure of the information.
   b. Electronic medical records data must remain accessible to authorized users for purposes of treatment, public health, patient safety, quality improvement, medical liability defense, and research.
   c. Physician and patient permission must be obtained for any person or entity other than the physician or patient to access and use individually identifiable clinical data, when the physician is specifically identified.
   d. Following the request from a physician to transfer his/her data to another data warehouse, the current vendor must transfer the electronic medical records and claims data and must delete/destroy the data from its data warehouse once the transfer has been completed and confirmed.

Our AMA: (1) will pursue the adoption of federal legislation and regulations that will: limit third party payers' random access to patient records unrelated to required quality assurance activities; limit third party payers' access to medical records to only that portion of the record (or only an abstract of the patient's records) necessary to evaluate for reimbursement purposes; require that requests for information and completion of forms be delineated and case specific; allow a summary of pertinent information relative to any inquiry into a patient's medical record be provided in lieu of a full copy of the records (except in instances of litigation where the records would be discoverable); and provide proper compensation for the time and skill spent by physicians and others in preparing and completing forms or summaries pertaining to patient records; and (2) supports the policy that copies of medical records of service no longer be required to be sent to insurance companies, Medicaid or Medicare with medical bills.

H-315.975, “Police, Payer, and Government Access to Patient Health Information”
(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 (CMMS) 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 CMMS 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.

H-315.979, “Electronic Data Interchange Status Report”
Our AMA will: (1) work to establish consensus on industry security guidelines for electronic storage and transmission of medical records as an important means of protecting patient privacy in a manner that avoids undue and non-productive burdens on physician practices; and (2) develop relevant educational tools or models in accordance with industry electronic security guidelines to assist physicians in compliance with state and federal regulations.

H-155.994, “Sharing of Diagnostic Findings”
The AMA (1) urges all physicians, when admitting patients to hospitals, to send pertinent abstracts of the patients' medical records, including histories and diagnostic procedures, so that the hospital physicians sharing in the care of those patients can practice more cost-effective and better medical care; (2) urges the hospital to return all information on in-hospital care to the attending physician upon patient discharge; and (3) encourages providers, working at the local level, to develop mechanisms for the sharing of diagnostic findings for a given patient in order to avoid duplication of expensive diagnostic tests and procedures.

H-315.977, “Abuse of the Medical Record for Regulation or Financing the Practice of Medicine”
1) Our AMA continues to oppose the use of the physician office medical record as a tool of CMS, as well as any other agency or third party, to regulate the financing and practice of medicine. (2) The medical record shall be the property of the physician and the information contained therein, the property of the patient. (3) The physician's office medical record should be used solely to document the delivery of health care.

H-315.971, “Patient Information in the Electronic Medical Record”
AMA Guidelines for Patient Access to Physicians' Electronic Medical Record Systems:

(1) Online interactions are best conducted over a secure network, with provisions for privacy and security, including encryption.

(2) Physicians should take reasonable steps to authenticate the identity of correspondent(s) in electronic communication and to ensure that recipients of information are authorized to receive it. Physicians are encouraged to follow the following guidelines for patient authentication: (a) Have a written patient authentication protocol for all practice personnel and require all members of the physician's staff to understand and adhere to the protocol. (b) Establish minimum standards for patient authentication when a patient is new to a practice or not well known. (c) Keep a written record, electronic or paper, of each patient authenticated.

(3) Prior to granting a patient access to his or her EMR, informed consent should be obtained regarding the appropriate use of and limitations to access of personal health information contained in the EMR. Physicians should develop and adhere to specific guidelines and protocols for online communications and/or patient access to the EMR for all patients, and make these guidelines known to the patient as part of the informed consent process. Such guidelines should specify
mechanisms for emergency access to the EMR and protection for and limitation of access to, highly sensitive medical information.

(4) If the patient is allowed to make annotations to his or her EMR (i.e., over-the-counter drug treatments, family medical history, other health information), the annotation should be indicated as authored by the patient with sourcing information (i.e., date and time stamp, login and IP address if applicable). A permanent record of all allowed annotations and communications relevant to the ongoing medical care of the patient should be maintained as part of the patient's medical record.

(5) Physicians retain the right to determine which information they do and/or do not import from a PHR into their EHR/EMR and to set parameters based on the clinical relevance of data contained within personal health records.

(6) Any data imported into a physician's EMR/EHR from a patient's personal health record (PHR) must preserve the source information of the original data and be further identified as to the PHR from which it was imported as additional source information to preserve an accurate audit trail.

(7) In order to maintain the legitimate recording of clinical events, patients should not be able to delete any health information in the record. Rather, in order to maintain the forensic nature of the record, patients should only be able to add notations when appropriate.

(8) Disclosures of Personal Health Information should comply with all applicable federal and state laws, privileges recognized in federal or state law, including common law, and the ethical requirements of physicians.

D-478.972, “EHR Interoperability”
Our AMA: (1) will enhance efforts to accelerate development and adoption of universal, enforceable electronic health record (EHR) interoperability standards for all vendors before the implementation of penalties associated with the Medicare Incentive Based Payment System; (2) supports and encourages Congress to introduce legislation to eliminate unjustified information blocking and excessive costs which prevent data exchange; (3) will develop model state legislation to eliminate pricing barriers to EHR interfaces and connections to Health Information Exchanges; (4) will continue efforts to promote interoperability of EHRs and clinical registries; (5) will seek ways to facilitate physician choice in selecting or migrating between EHR systems that are independent from hospital or health system mandates; and (6) will seek exemptions from Meaningful Use penalties due to the lack of interoperability or decertified EHRs and seek suspension of all Meaningful Use penalties by insurers, both public and private.