Federation of STATE MEDICAL BOARDS

Report of the Committee on Ethics and Professionalism in the Adoption and Use of Electronic Health Records

Adopted as policy by the House of Delegates of the Federation of State Medical Boards

April 2014

TABLE OF CONTENTS

Federation of STATE MEDICAL BOARDS

REPORT OF THE COMMITTEE ON ETHICS AND PROFESSIONALISM FRAMEWORK ON PROFESSIONALISM IN THE ADOPTION AND USE OF ELECTRONIC HEALTH RECORDS

EXECUTIVE SUMMARY

This framework seeks to assist providers in identifying issues that are likely to arise in the adoption and implementation of electronic health records ("EHRs"). Adherence to the recommendations contained in the document alone will not discharge a provider's ethical and professional obligations. Feedback received following the circulation of this document will be considered in developing a more comprehensive policy that may be accepted by the state boards as a reasonable standard of care in the implementation of electronic health records.

The Committee identified five separate issue areas providers are likely to encounter as they explore, adopt and move forward with implementation of electronic health records. The Committee also identified a number of ethically appropriate behaviors and related recommendations that will assist the state boards in ensuring their licensees are aware of the ethical and professional obligations EHR usage may trigger.

I. Implications of Adopting an Electronic Health Records System

Providers are advised first and foremost to seek expert advice to determine the system that best suits the needs and objectives of their practice.[1] Once a system has been selected, providers must consider how an EHR system is likely to impact patient encounters and seek to enhance patient-centered care. The Committee recommends that providers use desirable communication behaviors that may assist providers who use EHRs.

Recommendation 1:
When possible, a provider should seek to select the EHR system that best suits the needs and objectives of his or her practice. If the provider is not in a position to personally select the system, he or she should offer feedback regarding how well the system is serving his or her individual practice. Both organizations and providers should seek to adopt systems that will communicate efficiently with other systems, securely store protected health information ("PHI") and complement existing workflows and processes.

Recommendation 2:
Providers should consider adopting communication behaviors that will minimize the undesirable habits that may emerge after EHR implementation. Providers should take care to employ a thoughtful configuration in the exam room so that they may maintain more regular eye contact with patients and avoid making notations or attempting to communicate while their backs are turned to patients. To eliminate confusion or anxiety, providers should offer patients an explanation regarding how the introduction of a computer improves the interaction. This is particularly important when an EHR is introduced to an existing patient.

[1] *Specific objectives are set forth at the bottom of page 6 and top of page 7. These objectives are not conclusive and are intended to be a starting point for providers.*

II. Privacy, Confidentiality and Security

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is considered the primary codification of providers' legal obligations to protect patients' safety and confidentiality. The framework does not seek to supplant those obligations, nor diminish the importance of HIPAA's provisions; the framework instead seeks to illuminate the ways data breaches may occur, the types of safeguards that should be in place to prevent such occurrences, and to guide providers in their efforts to minimize consequences in the event of a breach. The Committee recognizes the value of audit trails and security audit policies and encourages providers to work with privacy officers and Health Information Management ("HIM") professionals to develop policies and procedures and educate staff accordingly. It is also necessary to educate patients so that they understand the limitations of their providers' technological use, the role electronic communication and other processes may play in the delivery of their care as well as their own roles.

Recommendation 3:
Providers should develop and adopt a security policy to prevent inadvertent disclosures of protected health information and remain HIPAA compliant. The policy should promote:

- Regular staff training;
- Ongoing internal audits;
- A response plan for incidents and investigations;
- Detailed risk assessments;
- Detailed records of the facts surrounding disclosures (particularly the dates of events).

The policy should be revisited to ensure its continued relevancy. Providers and staff should submit to ongoing training and education.

Recommendation 4:
In the event of a breach of data containing PHI, providers must promptly notify the patient, to whom the information belongs, disclosing the full scope of the breach. The provider should also assist in the mitigation of harm.

Recommendation 5:
Organizations and providers who use mobile devices in their practices must be prepared to educate patients on the limitations and risks of mobile device usage in the transmittal of health information and for other communicative purposes. Providers should consider adopting a written informed consent agreement to allow the provider and the patient to agree on the types of transmissions that will be permitted and are advised to develop a written policy to guide staff in their electronic communications with patients.

Recommendation 6:
Providers who make patient portals available to patients should take care to ensure the portal features the following elements:

- Secure messaging to alert patients to sign on when new information becomes available and the ability to send select questions to the provider;
- User authentication and role based authorization;
- High availability, scalability and configurability;
- Integration with an enterprise master patient index that allows patient matching and linking of records;
- Seamless integration with the provider's EHR system; and
- Ease of use for patients and providers.

Providers should consider the nature of the information when making it available through a patient portal. Information warranting an explanation or sensitivity should not be made available electronically.

Recommendation 7:
Where EHR systems present providers with research opportunities, informed patient consent is necessary. Providers should treat such opportunities as they would non-EHR research: careful vetting of the research, preliminary analysis and other precautions should be engaged in and observed in order to protect patient confidentiality and ensure patient autonomy.

III. Ethical Utilization of EHRs

As the adoption of EHRs have become more widespread and policymakers have sought to expand implementation, medical regulators have been grappling more and more with how to educate providers on the ethical obligations that arise from EHR usage. Seeking to increase efficiency and save time, providers may unknowingly engage in practices which violate their ethical or professional obligations. In the framework's "Ethical Utilization of EHRs" section, the Committee seeks to identify some common EHR practices that put the integrity of medical records and patient data at risk and may even contribute to adverse outcomes. This section also urges providers to anticipate and prepare for certain patient behaviors such as requests for access and amendments to the record. Access and amendments are required pursuant to HIPAA, thus it is imperative that these legal obligations are considered in the system selection, adoption and implementation processes.

Recommendation 8:
If a provider is satisfied that copying and pasting information into a new record entry is permissible in a given instance, he or she must include the appropriate citation in the record and verify that the copied information is current. Generally, it is inappropriate to copy and paste or otherwise document an entry that is not derived from a patient encounter at the time of the visit, unless the provider makes a clear notation that the information is copied and pasted from another record. Copy and paste is only appropriate when the content is verified. EHR systems should adopt processes that prevent indiscriminate and inappropriate copy and pasting. An EHR system should permit tracking of copying, pasting and other edits that occur within the record and effective audit strategy should be developed and used.

Recommendation 9:
Providers should explore and understand their system's authentication and electronic signature capabilities and functionalities and implement authentication policies and procedures to address, minimally, the issue of multiple or dual signatures, proxy signatures, auto-attestation functionality and batch signing.

Recommendation 10:
In utilizing an EHR system, providers must be mindful of anticipated patient behaviors and should seek to submit to systems and utilize features that allow for patient generated requests for access and amendments.

IV. Use of the EHR in Adjudication and for other Evidentiary Purposes

State medical boards and other investigative and adjudicative bodies rely upon information obtained from providers and organizations for many legal uses. The framework encourages providers to develop a written policy that

will assist providers and staff in determining the record that constitutes the appropriate disclosure. Providers are also urged to consider the efficiency of all possible rendering methods when making disclosures and be careful to include in the record, only information used by the practitioner in reaching a clinical judgment or opinion. Providers are responsible for any and all information included in his or her record. Information that is not used in reaching a clinical judgment should be returned to the patient or disclosed in a way that assures patient confidentiality.

The FSMB and the state medical boards are committed to ensuring patient safety and improving excellence in medical practice. These organizations understand that outcomes may be improved, patients may be better protected and greater efficiency may be achieved when well-developed EHRs are utilized appropriately. To assist providers in identifying patient safety goals, the Committee adopts the phases and principals included in the 2012 New England Journal of Medicine Article, "Electronic Health Records and National Patient Safety Goals." The NEJM framework includes suggestions to achieve each recommended goal and the Committee adopts the framework in full.

Recommendation 11:
Providers should make an effort to identify the set of records and/or information that comprise the legal health record for the purpose of disclosure and include the identified information in a written policy that is reflective of the services and setting in which care is provided and mindful of HIPAA's "minimum necessary" rule.

Recommendation 12:
To ensure EHR output produces valuable information, providers should be prepared to make review of the EHR screen available onsite or over remote, secure connections to ensure the disclosure of information necessary for investigations or e-discovery.

Recommendation 13:
Because providers are responsible for all information included in his or her record regardless of whether the information was generated by another provider in another encounter or presented by the patient, providers should be diligent in ensuring only information used by the provider in reaching a clinical judgment or opinion is included in the record. All other information should be returned to the patient or disposed of in a way that ensures patient confidentiality.

V. Patient Safety

The Committee recommends adopting the following phases and the principles encompassed therein. Each relevant element is set out below.

Recommendation 14:
Phase 1: Address safety concerns unique to EHR technology

1) Reduce the effect of EHR downtime on patient safety
2) Reduce miscommunication of data transmitted between different components of EHRs

Phase 2: Mitigate safety concerns arising from failure to use EHRs appropriately

1) Mandate computer-based provider order entry (CPOE) for all orders of medications, laboratory tests, and radiologic tests
2) Reduce alert fatigue whenever possible
3) Enter all medications, allergies, diagnostic test results, and clinical problems as structured or coded data

Phase 3: Use EHRs to monitor and improve patient safety

Use EHR-based "triggers" to monitor, identify and report potential safety issues and events.

REPORT OF THE COMMITTEE ON ETHICS AND PROFESSIONALISM FRAMEWORK ON PROFESSIONALISM IN THE ADOPTION AND USE OF ELECTRONIC HEALTH RECORDS

STUDY CHARGE

At the 2011 Federation of State Medical Boards' Annual Meeting, Resolution 11-2, Electronic Medical Records, was submitted for consideration by the FSMB House of Delegates. The Resolution emphasized the lack of standards and interoperability between then-current EMR systems and the difficulties and inefficiencies that so often result. The Resolution called on the FSMB to create a study process to inform and advise the state medical boards regarding the regulatory and functional implications of EMR systems and identify and recommend best practices. Careful consideration of the resolution resulted in the recommendation that the Board of Directors undertake a study process that would later lead to a more fully developed policy document. In conveying its support of an EHR project, the reference committee charged with the resolution's review acknowledged the resolution's broad scope and cautioned the Board of Directors to carefully consider the additional steps needed to properly prepare the policy document.

In 2012, the FSMB Board of Directors engaged in a process of preliminary study to determine how the FSMB should respond to the directives contained in Resolution 11-2. The Board produced a report summarizing what it believed to be an appropriate response. The strategy, the Board has posited, should include the following elements:

1) A comprehensive legal review of individual state statutes and regulations as they relate to EHRs;
2) Initiation of a dialogue with the American Health Information Management Association (AHIMA) for the purposes of collaborating to define a common legal EHR definition that can be recommended to state boards and other stakeholders;
3) Consultation with state medical boards and other stakeholders including the Federal Government, as appropriate, seeking guidance on a legal EHR definition;
4) Development of a model EHR policy that defines the standards of what constitutes a medical record for a regulatory board; and
5) Presentation of a model EHR policy at the 2013 FSMB Annual Meeting of the House of Delegates for review and adoption.

The Board of Directors referred the issue to the Committee on Ethics and Professionalism ("Committee") to develop recommendations for consideration by the state medical boards. Consistent with directives contained in the Board of Directors' 2012 report, representatives from AHIMA have served as subject matter experts to the Committee.

After lengthy discussion, the Committee concluded that a preliminary framework should precede the development of a later, more comprehensive policy document. The Committee identified five separate issue areas ripe for discussion and more than a dozen sub-issue areas.

The five primary issue areas this report seeks to address are:

1) Impact of Adopting an EHR system on the Physician-Patient Relationship;
2) Privacy, Confidentiality and Security;
3) Ethical EHR Behaviors;
4) Use of the EHR in Adjudication and for other Evidentiary Purposes; and
5) Patient Safety.

By exploring each of these issue areas and sub-issue areas, this report seeks to serve as the preliminary framework upon which a later policy document will be developed. This framework will be submitted to the state boards for comment and revised accordingly prior to presentation to the FSMB House of Delegates.

GLOSSARY

Though employing the appropriate terminology is always important, it is of critical importance when—as here—two principal terms are frequently, and somewhat inaccurately, used interchangeably. Electronic medical records and electronic health records are not synonyms though many in the health IT and medical industries use the terms interchangeably. Additionally, many of the terms employed by the health IT industry are not familiar and take on a very specific meaning in varying contexts. Thus, unless otherwise indicated, readers should refer to the glossary for definitions of terms contained in this framework.

Although Resolution 11-2 refers to electronic medical records (EMR), the Committee's use of the term electronic health records (EHR) is purposeful and in keeping with the current subtleties recognized between EMRs and EHRs.[2] Because this framework seeks to expand and improve interoperability between systems, a focus on EHRs—that are built to share information between health providers and systems—is appropriate.

Record of Care:
The record of care is also commonly referred to as the legal health record. It comprises all data and information gathered about a patient from the moment he or she enters the hospital/healthcare facility to the moment of discharge or transfer. As such, the record of care functions not only as a historical record of a patient's episode(s) of care, but also as a method of communication between providers and staff that can facilitate the continuity of care and aid in clinical decision making.[3]

Electronic Medical Record:
An electronic medical record (EMR) is a digital version of a paper chart that contains all of a patient's medical history from one practice. An EMR is mostly used by providers for diagnosis and treatment. [4]

Electronic Health Record:
Electronic health records (EHR) go beyond standard clinical data collected in the provider's office and are inclusive of a broader view on a patient's care. EHRs are designed to reach out beyond the health organization that originally collects and compiles the information. They are built to share information with other health care providers, so they contain information from all the clinicians involved in the patient's care. [5]

Audit trail:
Audit trails record key activities, showing system threads of access, changes and transactions and may be helpful for detecting disclosures of protected health information, reducing security risks and addressing compliance with regulatory and other requirements.[6]

---

[2] *Though many in the industry refer to EMRs and EHRs interchangeably, the Committee seeks to underline the difference between the two terms as it finds the distinction valuable. Primarily, the Committee seeks to emphasize the mobility of EHRs. EMRs are largely static documents that do not easily travel outside the practice. An EHR is designed to travel and includes information from all providers involved in the patient's care.*

[3] *The Committee adopts the Joint Commission's definition of record of care as articulated in January 2012.*

[4] *The Office of the National Coordinator for Health Information Technology (ONC), "What is an Electronic Medical Record (EMR)?" http://www.healthit.gov/providers-professionals/electronic-medical-records-emr*

[5] *ONC, "What are the differences between electronic medical records, electronic health records, and personal health records?" http://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference/*

[6] *AHIMA, "Security Audits of Electronic Health Information."*

Metadata:
Metadata, simply put, is "data about data."[7] It is data that may be viewed by users or hidden or embedded, which seeks to describe certain characteristics of electronically stored information that is found in different places and forms within an electronic system.[8] Metadata may offer details about electronically stored information such as how, when and by whom that information was collected, created, accessed and modified.[9]

IMPACT OF ADOPTING AN EHR SYSTEM ON THE PHYSICIAN-PATIENT RELATIONSHIP

While providers exploring the benefits of an operational and efficient EHR system may be persuaded by the possibility of broader, more immediate access to patients' health information; greater efficiency in their medical practice; and improved patient outcomes; providers must be prepared for possible challenges to implementation. Adopting an EHR system is a long-term commitment that requires diligent planning and will almost certainly present organizations and providers with new and somewhat novel issues during implementation. Some of these issues, while important, do not pose any risk to patient safety.

Spatial considerations, for instance, put patient satisfaction at risk, but will rarely—if ever—pose a threat to patient safety. While this framework seeks to identify key considerations in implementing an EHR system, the state boards' primary obligation is to the public. Consequently, this framework has a patient-centered focus. By highlighting the various ways the delivery of healthcare is likely to be affected by continued EHR expansion, the Committee seeks to assist providers in influencing the selection of appropriate EHR systems and avoiding EHR behaviors that may negatively impact patients or violate a provider's ethical or professional obligations.

A multitude of EHR vendors and systems exist today which present EHR consumers with nearly limitless options and functionalities. Organizations and providers are encouraged to identify the system that best suits the needs and objectives of their practice. The Committee is cognizant of the fact that employed providers practicing in an managed care setting are unlikely to be able to exercise autonomy over the EHR system that is selected; however, providers should seek to participate in the process when possible by serving on technology committees and communicating how well or how poorly the system serves his or her individual practice.

In order to contribute meaningfully to the EHR system dialogue, providers may find that more than a cursory knowledge of technology and informatics is required. Providers should ask the EHR vendor or organization's health information management (HIM) professional whether or how well the system: allows providers to communicate with other systems; store and record patient information; complements providers' workflows and processes and interacts with existing technological systems. To the extent a provider's existing knowledge is insufficient to make the aforementioned query, a provider may find that additional health information training or outside consultation is warranted.

Beyond considerations related to function and efficiency, providers should also be mindful of the practical consequences an EHR system is likely to have on clinical interactions. For instance, introducing a computer workstation to the exam room may mean that the practitioner's back is to the patient or the practitioner makes eye contact with the patient less regularly. Poor communication may impact patient satisfaction as well as patient outcomes, but can be avoided easily by wiser configurations. Providers may find that employing a triangle design, where the physician, patient and computer occupy each of the three corners, will allow the practitioner to look to the

---

[7] *AHIMA, "Rules for Handling and Maintaining Metadata in the EHR."*

[8] *The Sedona Conference, "The Sedona Conference Glossary: E-Discovery & Digital Information Management," www.thesedonaconference.org (2007).*

[9] *Id*

computer screen and the patient frequently without awkward pauses and movements.[10] Similarly, conscientious work-flow design will assist providers in employing superior communications skills.

Patients may be alarmed or confused by computer use in the exam room, particularly when the use is new to the interaction. However, providers may quell patients' fears by explaining how the introduction of a computer improves the interaction. For instance, providers should make a point to verbalize how the use of the computer allows the practitioner to see records from another provider during the visit or to send a patient's prescription directly to the pharmacy from the exam room. Patients may also be interested to see the screen and better understand the system. Providers should be prepared to let the patient look on and offer explanations as appropriate. For example, while making notations related to the visit, the provider may wish to thank the patient for their patience while he or she records important information relayed during the encounter. Making eye contact and communicating freely with the patient will give the patient assurance that you are using the limited time you have with them to provide quality care and not to finish up notations relating to another exam, check emails, etc.

Observing these simple communication behaviors may help to minimize the potentially negative effect a new EHR may have on the clinical setting; however, a practitioner's commitment to proper communication behaviors alone will not discharge the practitioner's responsibility to preserve and protect the physician-patient relationship. Providers have a responsibility to understand their EHR systems. At least one state has already codified this responsibility in its statutory code. In 2012, Massachusetts became the first state to require applicants for licensure to demonstrate proficiency in the use of computerized physician order entry, e-prescribing, EHRs and other forms of health information technology.[11] The provision provides that proficiency, at a minimum, requires applicants to demonstrate the skills to comply with the requirements of meaningful use as set forth at 45 C.F.R. Part 170.[12]

Recommendation 1:
When possible, a provider should seek to select the EHR system that best suits the needs and objectives of his or her practice. If the provider is not in a position to select a system, he or she should seek to influence the system by communicating how well the system is serving his or her practice. Organizations and providers alike should seek to adopt a system that will—at a minimum—communicate efficiently with other systems, securely store PHI and complement the provider's workflows and processes.

Recommendation 2:
It is the provider's responsibility to ensure that technology of all types does not interfere with the establishment of the physician-patient relationship and that communication behaviors are implemented to support patient care.

PRIVACY, CONFIDENTIALITY AND SECURITY

While it is true that developments in medical technology and the expansion of EHRs have presented providers and organizations alike with new privacy issues and considerations, protecting the privacy of patients has been recognized as an important ethical principle since the earliest stages of medical training. Some of the world's first physicians vowed:

---

[10] *American Medical News, "How to communicate well with a patient while working on an EHR," http://www.ama-assn.org/amednews/2012/07/23/bica0723.htm (2012).*

[11] *Massachusetts Senate, No. 2400, 187th 2011-2012, amending chapter 112 of the general laws, section 2.*

[12] *Id*

"Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all things to be private."[13]

By identifying ethically appropriate behaviors and responses to certain situations that may result from EHR system use, this document seeks to expand upon the well-established tradition of protecting patients' privacy and commitment to maintaining patients' confidentiality and trust while complementing the legal and regulatory framework that so clearly define providers' existing legal obligations.

Breach protection and reporting requirements

Providers and organizations that generate personal health information are committed to protecting that information from inappropriate or inadvertent disclosures. Most data breaches result from simple error. Laptops containing health information may be lost or stolen. Records may be released to the wrong person or a fax or mailing may be sent to the wrong address. Any number of inadvertent disclosures may result from improperly encrypted drives and files. All of these adverse outcomes may result from poor planning, poor training, recklessness, or mere forgetfulness. Simple, but strategic, security measures must be implemented to appropriately safeguard against inadvertent disclosures and are necessary to ensure compliance with HIPAA.[14] Appropriate steps should include, at a minimum, the following elements[15]:

1) Detailed security policies and procedures;
2) Regular staff education and training;
3) Ongoing internal audits;
4) A documented response plan for incidents and investigations;
5) Detailed risk assessments; and
6) Detailed records of the facts surrounding disclosures, particularly the dates of events

Adoption of these measures, collectively, will assist an organization or provider in assessing the adequacy of the data security system; however, a single, static exploration of each element will result in a quickly outdated and ineffective system. Organizations, providers and their properly designated privacy and security officer(s)[16] should examine and reexamine a practice's policies and procedures to ascertain their relevancy. Technological innovations are perpetual and require frequent evaluation. Training and education should also be ongoing.

Federal law requires certain responses in the event of a breach of data containing patient health information.[17] In addition to these statutory mandates, the Committee has identified a number of ethically appropriate responses.[18]

Notify the patient

After determining that a data breach has occurred and patient health information has been improperly accessed or disclosed, an organization, provider or privacy officer must promptly notify the patient to whom the health information belongs of the breach.

[13] *The Hippocratic Oath, National Library of Medicine, translated by Michael North, http://www.nlm.nih.gov/hmd/greek/greek_oath.html (2002).*

[14] *Implementation of these six identified elements alone will not be sufficient to discharge additional requirements mandated by HIPAA.*

[15] *AHIMA, "Keeping Compliant: Managing Rising Risk in Physician Practices."*

[16] *HIPAA requires designation of a privacy and security officer. 45 CFR § 164.530.*

[17] *See HIPAA and "breach notification" provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of the American Recovery and Reinvestment Act of 2009 (ARRA).*

[18] *The following comments are modified from American Medical Association (AMA) Opinion 5.10 available at http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion510.page.*

Make a proper disclosure

Merely notifying the patient of a breach involving his or her health information is insufficient to discharge the ethical obligations that arise when a breach occurs. Providers should also seek to minimize and mitigate harms that may result by making a prompt and thorough disclosure to the patient. The notification provided to the patient should contain a thorough description of the information improperly disclosed or accessed, including: what caused the breach to occur; known consequences, if any; corrective actions taken by the organization or provider; and what steps the patient might wish to take to mitigate additional harms.

The need to make additional information available may be triggered by applicable federal or state law. For instance, pursuant to the Breach Notification Rules of HITECH, the notification must also include the date of the breach, the date of discovery (if known) and contact information. There may be further requirements based on the circumstances of the breach and the state within which the breach occurs.

Providers are reminded that the dignitary harms that may result from a breach can have serious consequences on the physician-patient relationship and that it is imperative that an open dialogue exist in the wake of a breach. Depending upon the circumstances of the breach, providers should be prepared to take action that will allow the patient to regain trust in the provider and the process. Research indicates many patients seek an apology from the provider or organization following a breach; others seek affirmation that corrective actions have been taken to assure similar breaches or events will not occur in the future.

Assist in the mitigation of harm

As fully as possible, the organization or provider should seek to assist the patient in responding to the breach. An appropriate response will require that the patient be made aware of the full range of possible consequences. The organization or provider is best suited to determine the scope and impact of the breach and should assist the patient in determining what actions must be taken in order to minimize or mitigate harms. In some circumstances, affirmative assistance may be proper, such as credit monitoring services, an identity theft hotline, etc.

Use of security audits and audit trails

Implementation of a security audit policy will allow organizations, providers and their properly designated privacy officers to monitor disclosures and detect potential breaches and other security risks. The use of audit trails and audit logs is necessary in order to maintain HIPAA compliance. The EHR system must allow amendments which will generally require that the system have the ability to track corrections and signal when an original entry has been modified. Not only should the original entry be viewable, but a date and time stamp, author of the modification and reason for the modification must also be noted.[20]

The audit trail should identify amendments—including deletions—as well as metadata such as the name of the user, the application triggering the audit, the workstation, the document title, a description of the event, and the date and time.[21] Even if no amendments are made, the event description should specify when the document has been viewed and whether it was printed, edited, etc.

Patient engagement and expectations

It is estimated that in 2013, mobile devices will outnumber personal computers.[22] With such ready access to tools that promise to improve existing encounters and enable altogether new ones, health care consumers will

[20] *Id.*

[21] *Id.*

[22] *The NPD Group/Connected Intelligence, "Connected Home Report." https://www.npd.com/wps/portal/npd/us/news/press-releases/more-than-400-million-devices-are-connected-in-us-homes-according-to-the-npd-group/ (2012).*

continue to expect more and more ready access to providers through emails, smart phones, tablets and Skype-like technology. The use of these technologies may result in convenience and more immediate access, but it also involves a degree of risk. If a mobile device is used to generate a record of care: where is that information stored? Is it accessible to other providers and patients? If emails are used to exchange information between providers and patients or between providers in the same system: are such exchanges prohibited by organizational policy? Are the systems secure? If the transmission includes PHI or diagnosis or treatment information, does it automatically become a part of the record?

When determining whether to enhance an existing system with the use of mobile devices, a practitioner should carefully consider the ethical issues raised and observe the safeguards necessary to fulfill any resulting ethical or professional obligations.

Engaging the patient

In 2012, the Office of the National Coordinator for Health Information Technology released its "Patient Engagement Framework" which was produced in an effort to assist healthcare organizations in the development of effective patient engagement strategies.[23] The framework promotes the use of eHealth tools and resources[24] as a powerful engagement tool while subtly communicating the proper role eHealth tools, resources and other devices might play in a secure practice. To the extent the limitations of eHealth tools and devices conflict with patient expectations, it is important that providers communicate why a particular use must be limited. For example, if the patient seeks to transmit an image of a skin condition by text message to the practitioner's mobile device, the practitioner should explain that the photo qualifies as protected health information which cannot be transmitted via an unsecured device such as a cell phone. The practitioner should explain that these limitations are intended to, and do in fact, serve to protect the confidentiality and privacy of the patient.

Electronic communications

Providers, like all professionals, rely heavily on the convenience and near real-time access provided by email and other electronic communications. Patients also, rely on electronic communications in their professional and personal lives and are not likely to anticipate the ethical dilemma they may pose for providers. Thus, it is important to communicate the limitations of electronic communications—including risks to privacy and confidentiality—and if necessary, temper patients' expectations. Providers may find that implementing an electronic communication policy and seeking to obtain patients' informed consent before transmitting health information by email, online or through social media, are simple and highly effective tools for operating within the parameters providers find comfortable and secure.

Though this framework fails to identify every element that should be considered when contemplating the development of an electronic communications policy, the FSMB has produced two policy documents that may be instructive. The FSMB's "Model Guidelines for the Appropriate Use of the Internet in Medical Practice" address appropriate electronic communication practices. The FSMB's *Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practice* highlights issues that are likely to be encountered by providers in their use of social media, including: discussing medicine online, protecting patients' privacy and confidentiality, and online interactions with patients.

A written informed consent agreement will allow the practitioner and patient to agree on the types of transmissions that will be permitted (prescription refills, appointment scheduling, patient education, etc.); under what

[23] *National eHealth Collaborative (NeHC), "The Patient Engagement Framework," http://www.nationalehealth.org/patient-engagement-framework (2012).*

[24] *eHealth refers to technologically enabled healthcare practices and tools like such as telemedicine and EHRs.*

circumstances alternate forms of communication or office visits should be utilized; security measures such as encrypting data, password protected screen savers and data files, or utilizing other reliable authentication methods, as well as potential risks to privacy; and requirements for express patient consent to forward PHI to a third party. Patients should be encouraged to confirm that they have received and read all messages and email systems should be configured to include an automatic reply to acknowledge message delivery and indicate that messages have been read. All patient-physician email, as well as all other patient-related electronic communications, should be stored and filed in the patient's medical record. A reasonable response time should be established for patient-physician email exchanges and alternate forms of communication should be identified in the case of an emergency. It is critically important to implement security measures that will adequately protect the confidentiality and integrity of PHI.[25] All transmissions (email, prescriptions, laboratory results, etc.) must ideally occur over a secured system featuring password protection, encrypted electronic prescriptions and other available authentication methods.

A written practice policy guiding staff and other providers who might reasonably seek to interact with patients via electronic communications may be beneficial and should seek to address the following issues:

1) Privacy, security, and confidentiality;
2) Health-care personnel (including providers) who will process messages;
3) Hours of operation;

4) The nature of information that may be exchanged and the types of electronic transactions that will be permitted;
5) Required patient information to be included in the communication, for instance, patient name, identification number and type of transaction;
6) Archival and retrieval; and
7) Quality oversight mechanisms.

Providers in an institutional setting should consult the organizational policy in place to ensure that he or she is properly operating within any identified parameters. As is the case with any policy or procedure, the organization, provider or properly designated privacy and/or security officer should assess the policy's efficacy often to ensure its relevancy.

Patient portals

Patient portals, accessible through the internet, enable patients to more actively engage in their health care by providing what is typically a subset of information from the patient's record such as diagnostic test results, medication lists and summaries of care. Patient portals may offer the functionality to view or download information from the portal into a patient maintained personal health record. Additional functionality may include the ability to schedule appointments, view bills, receive alerts and reminders for preventive and follow up care, receive specific educational materials and increasingly, ask a variety of questions about the information provided, including those about the nature and accuracy of their health information. When designed and used properly, patient portals have the potential to enhance patient engagement in their care. According to health care information security and information technology experts, key features of a patient portal should include:

[25] *FSMB, "Model Guidelines for the Appropriate Use of the Internet in Medical Practice," (2002).*

- Secure messaging to alert patients to sign on when new information becomes available and the ability to send select questions to the provider;
- User authentication and role based authorization;
- High availability, scalability, and configurability;
- Integration with an enterprise master patient index that allows patient matching and linking of records;
- Seamless integration with the provider's EHR system;
- Data encryption; and
- Ease of use for both patient and clinicians.

One of the most attractive features of patient portals is the around-the-clock access to information. Patients may access information through a patient portal at their convenience, and will often log-in after hours when a provider is not available to answer questions or discuss a result or other information. Accordingly, providers should properly prepare patients for certain types of information that may be viewable through a patient portal or make sensitive information unavailable until the provider is able to speak with the patient directly.

Research implications

The EHR provides opportunities for tracking and research regarding care practices and patient behavior. This information may be helpful within practices to assist with individual patient care and education and within practices where recurrent issues may lead to behavior change for health care providers or educational opportunities across the population of patients served. Where research opportunities exist across EHR systems, patient consent for participation is essential. As with non-EHR research, consent for participation in particular research must be carefully vetted and opportunities for generic consent to participation in future research must be carefully analyzed. Patient identifiers should be eliminated. Also, where patterns of illness or intervention are being studied across patients in an EHR, implications of findings that may impact particular patients should also be explored.

Recommendation 3:

Providers should develop and adopt a security policy to prevent inadvertent disclosures of PHI and remain HIPAA compliant. The policy should promote:

- Regular staff education and training;
- Ongoing internal audits;
- A response plan for incidents and investigations;
- Detailed risk assessments; and
- Detailed records of the facts surrounding disclosures (particularly the dates of events).

The policy should be revisited by organizations, providers and their privacy designees to ensure its continued relevancy.

Recommendation 4:

In the event of a breach of data containing PHI, providers must promptly notify the patient to whom the information belongs, disclosing the full scope of the breach ensuring compliance with all breach notification requirements under the law. The provider should also assist in the mitigation of harm.

Recommendation 5:
Organizations that permit—and providers who elect—to use mobile devices in their practices must be prepared to educate patients on the limitations and risks of mobile device usage in the transmittal of health information and for other communicative purposes. Providers should consider adopting a written informed consent agreement to allow the provider and the patient to agree on the types of transmissions that will be permitted and are advised to develop a written policy to guide staff in their electronic communications with patients.

Recommendation 6:
Providers who make patient portals available to patients should take care to ensure the portal features the following elements:

- Secure messaging to alert patients to sign on when new information becomes available and the ability to send select questions to the provider;
- User authentication and role-based authorization;
- High availability, scalability and configurability;
- Integration with an enterprise master patient index that allows patient matching and linking of records;
- Seamless integration with the provider's EHR system; and
- Ease of use for patients and providers.

Providers are advised to consider the nature of the information when making it available through a patient portal. Information warranting an explanation or sensitivity should not be made available electronically.

Recommendation 7:
Where EHR systems present providers with research opportunities, informed patient consent is necessary. Providers should treat such opportunities as they would non-EHR research: careful vetting of the research, preliminary analysis and other precautions should be engaged in and observed in order to protect patient confidentiality and ensure patient autonomy.

ETHICAL UTILIZATION OF EHRS

Provider behaviors

Providers have an ethical obligation to ensure the integrity of the medical records they author. Ensuring integrity requires that documentation accurately reflect the author's encounter with the patient and the information that served as the basis for decision making about patient care at that encounter. Providers are under constant pressure to remain compliant with ever-evolving regulations, to respond to new technologies, increase efficiency and provide quality care. These objectives may cause providers to engage in behaviors they believe will save time, but which are in fact, unethical, unprofessional or unsafe. Knowledge of how the EHR operates as well as observation of certain simple, minimum standards can be quite effective in maintaining the integrity[26] of medical records data.

Copying and pasting
Providers may be tempted to utilize the copy/paste functionality in an effort to maximize efficiency in spite of or without knowledge of the risks posed by copying and pasting records from an earlier encounter. Providers must take note of the following risks which are often triggered by utilization of this functionality:

1) Copying information into the wrong patient health record;

[26] *Data integrity requires, at a minimum, that the records comprising a provider's data remain unaltered from their original form and free from unauthorized access.*

2) Noting inaccurate or outdated information;
3) Including redundant information, which hinders current and future providers' ability to determine current information;
4) Inability to identify the author or intent of documentation;
5) Inability to identify when the documentation was first created;
6) Inability to accurately support or defend E/M codes for professional or technical billing notes;
7) Propagation of false information; and
8) Internally inconsistent progress notes.[27]

These risks, collectively or independent of one another, could adversely impact patient care as well as put the provider at risk for fraud under federal payment programs such as Medicare and Medicaid. Accordingly, the Committee recommends caution in the use of copy/paste functionality. The Committee does not seek to prohibit the use of this functionality altogether as it may be appropriate in certain circumstances. For instance, copied information may be appropriate when based on external and independently verifiable sources that are stable over time. Examples of independently verifiable information include: demographics, medications, allergies, problems and labs and treatment or therapies. Copied information may also be appropriate in instances "when the information is clearly and easily distinguished from original information, such as automatic summaries that populate data fields, are clearly identified as non-original, and cannot be mistaken for original information."[28] If the provider is satisfied that copying is appropriate, it is imperative to include the appropriate citation in the record and verify that all copied information is current.

The Committee recognizes that copying and pasting may be a means of expediting medical records documentation; however, it is unethical and inappropriate to "copy and paste" or otherwise document an entry that is not derived from a patient encounter at the time of the visit without indicating that the information is copied and pasted from another record. The Committee supports efforts to promote functionalities that enable an indication that copying, pasting, and other edits have occurred.

A number of alternatives to copy functionality exist which may foster greater provider productivity while maintaining the integrity of the medical record. For instance, dictation, transcription, voice recognition and medical scribes allow a provider to contribute information to the medical records without entering information. Systems that allow citations from a problem list or medications list and to allergies and current labs may also result in time savings, as may templates with drop down menus and check boxes and macros that include routine phrases that may be populated automatically, however physicians should take care to ensure they are not documenting work they did not perform. Providers are advised to consult an expert to determine appropriate use of these features in their current EHR system. In considering an EHR system and vendor, providers should ascertain how best to use these features when they are available.

Authentication

The authentication process in health IT differs slightly from the traditional authentication act of signing an electronic entry. In an EHR system, the authentication process has two main objectives: 1) to verify a user's identity within the system; and 2) to confirm that the user should have access to the system.[29] Appropriate access refers to a user's ability and responsibility to create, modify or view an electronic entry and will require research into individual states' regulation of e-signature practices as state and federal rules and regulation are likely to differ with respect to context as well as issue. For instance, administrators and HIM professionals may choose to implement

[27] *Additional considerations exist, which are not inherently ethical, but which may complicate the delivery of healthcare nonetheless. Among those considerations worth mentioning are: overuse of storage space that may reduce overall system performance/response time and unnecessarily lengthy progress notes.*

[28] *Id.*

[29] *AHIMA, "Information Integrity in the Electronic Health Record."*

practices and policies that strive to preserve signature integrity in case of investigative or adjudicative need, such as a subpoena, or even resident accountability, if the organization is a teaching facility.[30] Authentication practices and policies should address, at a minimum, issues such as multiple or dual signatures, proxy signatures, auto-attestation functionality and batch signing. Likewise, providers and HIM professionals should explore and understand their system's authentication and electronic signature capabilities and functionalities.

Confirming the identity of the patient

Although there are no specific verification practices required by law, providers must engage in good faith measures to verify the identity of any person requesting PHI as well as all persons who will have access to the information. To discharge this obligation, a provider may choose to ask for photo identification or compare a signature to an existing signature on file.[31] Providers should also consider developing a customer-friendly script for requesting PHI and verification information; defining a set of attributes that will be used consistently for identifying and verifying identities; building effective business processes and quality checks with clear standards, policies and procedures into identification activities; and collecting additional data elements, such as mother's maiden name.[32]

Patient behaviors

Providers should submit to systems and generate records which are compatible with anticipated patient behaviors. Patients are likely to continue to seek greater access to their records and are legally entitled to obtain copies of their medical records and request amendments pursuant to HIPAA and HITECH.[33] Providers should keep these objectives in mind when selecting systems and should adopt policies that allow for reasonable access and requests for amendments by patients.

Access

The benefits of patient access are well documented and depend upon greater patient autonomy and physician transparency. Providers' ethical obligation to ensure patient access to personal health information is protected by federal regulation in the HIPAA Privacy Rule and elsewhere in federal and state law. The Privacy Rule generally grants individuals a right to inspect and obtain "protected health information about the individual in a designated record set (DRS)."[34] The Rule is directed to "covered entities" which includes providers, health plans, and clearing houses that transmit information in an electronic form in connection with a transaction for which the United States Department of Health and Human Services (HHS) has adopted a standard.[35]

Providers have long struggled to define the designated record set though a definition is included in the HIPAA Privacy Rule.[36] It is imperative that the DRS is clearly defined for each covered entity. The defined DRS is used to clarify the rights of individuals to access, amend, restrict, and acquire an accounting of disclosures. Individuals have the right to inspect and obtain a copy, request amendments, and set restrictions and accountings of medical and billing information used to make decisions about their care. Under HIPAA, the DRS is defined as a group of records maintained by or for a covered entity that may include:

---

[30] *AHIMA, "The Legal Process and Electronic Health Records."*

[31] *AHIMA, "The Privacy and Security of Occupational Health Records."*

[32] *AHIMA, "Limiting the Use of the Social Security Number in Healthcare."*

[33] *45 CFR § 164.524(a)(1).*

[34] *Id.*

[35] *U.S. Department of Health and Human Services, "For Covered Entities and Business Associates," available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.*

[36] *45 CFR § 164.501(1).*

- Patient medical and billing records;
- Enrollment, payment, claims, adjudication;
- Cases or medical management record systems maintained by or for a health plan; or; and
- Information used in whole or in part to make care-related decisions.[37]

Requesting amendments to the record

Though providers may have reason to amend the record either by correcting or deleting certain information contained therein, patients have a legally protected right to request amendments of the information comprising their health record. Organizations and providers should develop policies and procedures to govern these requests, including how requests should be submitted, what information should be included in a request and how quickly a provider must respond.[38]

HIPAA provides, in greater detail, covered entities' obligations with respect to a patient's request for an amendment; thus further explanation is not warranted in this text. However, organizations and providers must ensure that their EHR systems will support the appropriate responses to patient requests, including making the appropriate notation in the EHR so that amendments are properly recorded and communicated in future transmissions.[39] Depending upon the resolution of the request, additional documentation—a letter of disagreement, for instance—should be included in the record.

Recommendation 8:

When utilizing the copy functionality, a provider should be careful to include the appropriate citation in the record and verify that the copied information is current. Generally, it is inappropriate to copy and paste or otherwise document an entry that is not derived from a patient encounter at the time of the visit, unless the provider makes a clear notation that the information is copied and pasted from another record. Copy and paste is only appropriate when the content is verified. EHR systems should adopt processes that prevent indiscriminate and inappropriate copy and pasting. The EHR system should permit tracking of copying, pasting and other edits that occur within the record and an effective audit strategy should be developed.

Recommendation 9:

Providers should explore and understand their system's authentication and electronic signature capabilities and functionalities and implement authentication policies and procedures to address, minimally, the issue of multiple or dual signatures, proxy signatures, auto-attestation functionality and batch signing.

Recommendation 10:

In utilizing an EHR system, providers must be mindful of anticipated patient behaviors and should seek to submit to systems and utilize features that allow for patient generated requests for access and amendments.

---

[37] *Id*

[38] *HIPAA requires that providers must provide responses within 60 days of receiving the request. A one time 30 day extension may be available if needed.*

[39] *See "Use of Security Audits and Audit Trails," page 6.*

USE OF THE EHR IN ADJUDICATION AND FOR OTHER EVIDENTIARY PURPOSES

Defining the Record of Care

Providers and organizations are likely to encounter requests for health information for use in investigations, subpoenas, adjudication, and other legal uses. If appropriately defined, the legal health record (LHR) will constitute the appropriate response to most requests. The HIPAA Privacy Rule contemplates the LHR, but fails to include a definition. As a result, providers and organizations may have difficulty drawing proper distinctions between the LHR and the designated record set (DRS) and what information should be included in each record. This is an important task as individual state and federal regulations differ with respect to retention, statute of limitations, and other important requirements.

Although "legal health record" is employed in HIPAA, legal professionals have taken issue with the rigidity of the term and many have advocated use of the less legally operative term, "record of care." For the purposes of this document, the Committee believes "record of care" should be used in lieu of "legal health record" to describe the data and information gathered about a patient from the moment he or she enters the hospital/healthcare facility to the moment of discharge or transfer. Generally, the record of care may be understood to comprise the provider or organization's business record. It consists of all the patient-specific data that is accumulated by a provider in the course of treatment though the inclusion of external information will often also be necessary.[40] Under HIPAA, organizations must include any external information used in current clinical decision-making.[41] It is often difficult to gauge how heavily past information weighs or should weigh on a current clinical judgment. Policy and practices must be developed to guide staff in identifying the full scope of internal and external information to be included in the record of care. Policies should also address how to properly store or dispose of external information that does not become part of the record of care.

Currently, there are no uniform standards that specify what constitutes the official health record for purposes of disclosure. Providers and organizations should identify the set of records and/or information in a written policy that can be used to guide authorized or otherwise appropriate disclosures. The policy should be reflective of the type of clinical services and setting in which care is provided. For example, a hospital stay typically involves the generation of a discharge summary which would be part of the disclosure set for a hospital; however, discharge summaries are not found in a clinic or outpatient setting though a clinic note would be.

With an EHR, identification of the official record for disclosure can be particularly challenging since these systems contain data and information not found in paper-based systems. Data may be found both in the EHR and a feeder or source system for the EHR such as a laboratory information system (LIS). It is important to identify which will be used for disclosure purposes.

Data such as clinical decision support rules, alerts and reminders; value sets; audit trails and metadata tags can provide additional potentially useful information depending on the purpose of the disclosure such as those for e-discovery and e-forensics. At the present time, we would advise that this type of electronically stored information (ESI) not be included as part of the official record; however, exclusion in a written policy does not preclude or prevent this information from being disclosed for evidentiary purposes in investigations and litigation.

---

[40] *AHIMA, "Information Integrity in Electronic Health Records."*

[41] *45 CFR §164.501(1)(iii).=*

Although encouraged to define in policy the official record for purposes of disclosure, providers must always be mindful of the 'minimum necessary' rule under HIPAA[42] and make disclosure only for requests that specify the identification of the patient and provider (if appropriate); the dates for which information is needed, and the specific purpose for which the information will be used. This information, along with a pre-defined organizational policy will allow most requests for disclosures to be filled appropriately.

Output from EHRs

Output from EHRs may be rendered as either a computer screen display, a downloaded file in various formats such as .pdf, .jpeg or .tiff (for images), or as printed paper. Many EHRs can present a variety of views in any of these rendering methods, depending on the access rights of the person requesting the output and it is not uncommon to receive different views of the same information at different times. Paper output particularly can be problematic since some EHRs are not designed with printing in mind, often producing voluminous amounts of paper with little useful information. Until EHR vendors make paper printouts more useful, it may be necessary to review computer screen displays either onsite or over remote, secure connections to produce information needed for disclosures involving investigations or e-discovery.

State medical boards seeking records for investigative or adjudicative purposes have found that information in EHRs may be brief in comparison to handwritten notes. The templates in EHRs often capture information with checkboxes and when additional documentation is possible, character or text limits are not uncommon. Providers should be careful to produce records which adequately support the course of treatment taken. This may necessitate that providers supplement the EHR with additional treatment notes that adequately detail the encounter and unique factual or situational elements leading to the proposed treatment or resolution of the medical case. Review of existing regulation may be warranted to ensure EHRs and EHR-specific record requirements are contemplated. For instance, regulation requiring providers to create and preserve an adequate record of treatment may be amended to specify that the requirement applies to EHR and traditional records indiscriminately.

Inclusion of external information in EHRs

A provider is responsible for any and all information included in his or her record, irrespective of whether the information was generated by another practitioner in another encounter or presented by the patient. Thus providers should be careful to include in the record, only information used by the practitioner in reaching a clinical judgment or opinion. All other information should be returned to the patient or disposed of in a way that ensures patient confidentiality. Information received from a referring practitioner that was used in providing care may be scanned and saved in a part of the EHR which clearly identifies that it came from the patient or an outside provider's record. This type of information may typically be marked as "correspondence" or otherwise indicated to originate from an outside source.

Recommendation 11:

Providers should make an effort to identify the set of records and/or information that comprise the legal health record for the purpose of disclosure and include the identified information in a written policy that is reflective of the services and setting in which care is provided and mindful of HIPAA's "minimum necessary" rule.

Recommendation 12:

To support that EHR output produces valuable information, providers should be prepared to make review of the

[42] *The minimum necessary rule provides that covered entities must take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. 45 CFR 164.502(b).*

EHR screen available onsite or over remote, secure connections to ensure the disclosure of information necessary for investigations or e-discovery.

Recommendation 13:
Providers are responsible for all information in his or her record, regardless of the source. Providers should be diligent in ensuring all information relied on in clinical decision making be included in the record. Any unused information should not be incorporated into the medical record and returned to the patient or disposed of in way that protects patient confidentiality.

PATIENT SAFETY

As providers continue to adopt technology into their medical practices in new and innovative ways, it will become more and more important to identify best practices and guide physicians and allied health providers in the appropriate use of technology. Information and data integrity assures the reliability, dependability, and trustworthiness of information and data that includes how, when, where and why such information is recorded, processed, saved, shared, used, safeguarded and stored. A lack of understanding of the skills and knowledge of health information management or information technology and the mechanics of EHR use may not be an adequate guard against board action involving health care providers who implement and use EHR systems to deliver and record health care. The state medical boards' mandate to protect the public through the regulation of the practice of medicine necessitates that the state boards take an interest in any issue that involves patient safety. When utilized correctly, EHRs and other technologically enabled medical practices may improve patient safety by giving providers access to complete and accurate information. By contrast, improper EHR practices may diminish the amount of time providers have to spend with their patients, contribute to adverse outcomes and subject patients to dignitary harms.

The Committee acknowledges that sound policy, though necessary, can be difficult to promulgate due to the rapid speed with which technological innovations occur, are offered and implemented. Policy and regulatory developments are complicated by the highly varied pace organizations, institutions and providers adopt EHR systems. A 2012 article from the *New England Journal of Medicine* (NEJM) titled, "Electronic Health Records and National Patient Safety Goals," effectively illuminates the safety benefits and risks inherent in EHR adoption and identifies three phases of implementation. The Committee recommends adopting all three phases and the principles encompassed therein. Each relevant element is set out below.

Recommendation 14:
Phase 1: Address safety concerns unique to EHR technology

3) Reduce the effect of EHR downtime on patient safety
4) Reduce miscommunication of data transmitted between different components of EHRs

Phase 2: Mitigate safety concerns arising from failure to use EHRs appropriately

4) Mandate computer-based provider order entry (CPOE) for all orders of medications, laboratory tests, and radiologic tests
5) Reduce alert fatigue[43]
6) Enter all medications, allergies, diagnostic test results, and clinical problems as structured or coded data

[43] *Alert fatigue refers to the dulled response health care providers experience as a result of excessive automated warnings about items such as possible dangerous drug interactions and other potential adverse reactions.*

Phase 3: Use EHRs to monitor and improve patient safety

Use EHR-based "triggers" to monitor, identify and report potential safety issues and events.

Included in the *NEJM* framework are suggestions to achieve each recommended goal. The Committee strongly recommends that the Boards consult the *NEJM* framework, and consider adopting the elements contained therein. The Committee has identified a number of additional organizational resources that may assist the boards in educating their licensees.

American College of Physicians

The American College of Physicians (ACP) has developed an EHR adoption roadmap to guide providers in EHR adoption. The ACP recognizes three stages of EHR adoption and has developed a number of guides, tools and references which may be accessed online at http://www.acponline.org/running_practice/technology/ehr/.

Institute of Medicine

The Institute of Medicine (IOM) has produced meaningful materials on the unintended consequences of EHR adoption.

Office of the National Coordinator for Health Information Technology

The Office of the National Coordinator for Health Information Technology's (ONC) Guide to Reducing Unintended Consequences of Electronic Health Records, is a valuable tool that seeks to prepare all types of health care organizations for the issues that may arise when implementing EHRs. The Guide is an online tool available at http://www.healthit.gov/unintended-consequences/content/module-i-introduction-unintended-consequences.html.

CONCLUSION

EHRs have changed how providers deliver healthcare, from the way records are generated, to the way clinical interactions occur. In addition to changing the way patients consume their health information, EHRs heighten their expectations regarding access, privacy and confidentiality. To ensure public protection in this rapidly evolving environment, state boards must identify best EHR practices, promulgate sound policy and communicate the resulting ethical and professional obligations to their licensees.

Increased EHR adoption affects the everyday practices of the state boards. In response to records requests, state board staff will inevitably receive output from EHRs, which may require yet to be determined formats or even remote access. The boards must familiarize themselves with state and federal regulation governing EHRs so as to properly evaluate the providers' usage. Perhaps most importantly, the boards must understand the practical effect EHR usage is likely to have on the physician-patient relationship, so that they can educate providers accordingly and promote practices that will adequately protect the public. For example, harm through the propagation of false information by utilizing the copy functionality may not be readily apparent, but the risk to patients is very real. The duty of adjudicating these issues and considerations belongs to the state boards. In developing this framework, the Committee seeks to assist the boards with this important task.

To ensure that patients are adequately protected and providers are given the guidance they need to meet all professional obligations, the state boards should begin examining this issue in earnest and articulate standards

as soon as practicable. Thus, this framework also seeks to serve as a preliminary policy document to guide the boards in their discussion and eventually, serve as the basis for a comprehensive policy document that can be adopted in full or in part by the boards.

POSSIBLE ALLIANCES

The Committee believes that the following entities, based on expertise or mutual interest, may be able to contribute meaningfully to this framework and any subsequent policy document. Accordingly, the Committee recommends that the FSMB contact these organizations and begin exploring the various ways an alliance may be formed.

- American Health Information Management Association (AHIMA)
- FSMB Foundation
- American Osteopathic Association of Medical Informatics (AOAMI)
- American Medical Informatics Association (AMIA)
- American College of Physicians (ACP)
- Office of the National Coordinator for Health Information Technology (ONC)
- Healthcare Information and Management Systems Society (HIMSS)
- Centers for Medicare and Medicaid Services (CMS)
- American Medical Association (AMA)
- American Osteopathic Association (AOA)

COMMITTEE ON ETHICS AND PROFESSIONALISM

Janelle A. Rhyne, MD, Chair
Former Chair, North Carolina Medical Board
Past Chair, Federation of State Medical Boards

Rev. O. Richard Bowyer, MDiv
Public Member, President, West Virginia Board of Medicine

Leslie M. Burger, MD
Member, Washington State Medical Quality Assurance Commission

Constance G. Diamond, DA
Public Member, New York State Board For Medicine

Gerald T. Kaplan, MA
Public Member, Minnesota Board of Medical Practice

SUBJECT MATTER EXPERTS

Kathleen Kinlaw, MDiv
Emory University Center for Ethics

Angela Dinh Rose, MHA, RHIA, CHPS
The American Health Information Management Association

Lydia Washington, MS, RHIA, CPHIMS
The American Health Information Management Association

Bruce D. White, DO, JD
Alden March Bioethics Institute

EX OFFICIOS

Jon V. Thomas, MD, MBA
Chair, FSMB

Donald H. Polk, DO
Chair-elect, FSMB

Humayun J. Chaudhry, DO, MACP
President and CEO, FSMB

STAFF SUPPORT

Lisa A. Robin, MLA
Chief Advocacy Officer, FSMB

Shiri Hickman, JD
State Legislative and Policy Manager, FSMB

(817) 868-4000 | www.fsmb.org