advance for Health Information Executives

HIPAA: An Opportunity for Continuity of Care

By Stephen L. Priest, FHIMSS, CPHIMS

Health care entities and their associates should be embarrassed.

Many are not wholeheartedly supporting and enthusiastically implementing HIPAA security.

Health care entities and HIPAA trainers often present HIPAA as "another federal regulation requiring compliance." Instead, HIPAA should be loudly proclaimed from the treetops as an opportunity to make real the promise of continuity of care.

The embarrassment

Most Americans believe their health records are shared among their health care providers, and that technology is increasingly being used to maintain and transfer their health information. However, consumers also recognize a need to protect the confidentiality and security of each individual's health information. In addition, clinicians have been skeptical in giving up the paper record for concern that the electronic health record (EHR) might not be readily available in a timely manner. In effect, we have an ongoing clash between consumers with their concern for confidentiality and security of their health information, and clinicians with their concern for the availability of the EHR.

In his *Escape Fire –Lessons for the Future of Healthcare*, Don Berwick, MD, readily articulates that we need for patients and providers to talk one-on-one; however, that communication will not eliminate the estimated 98,000 annual preventable inpatient deaths identified in the Institute of Medicine study, *To Err is Human*. Clinicians are not doing a good job communicating patient information with each other. They talk with the patient, but their piece of the pie is not effectively integrated into the whole patient picture.

When multiple clinicians, such as physician specialists and consultants, nurses, therapists, dieticians and technicians, are involved in the care of a patient, often the left hand does not know what the right hand has done, or is doing. A simple example is when a drug causes an allergic reaction: As others are brought into the case, there may be a repeat of the drug -- and reaction -- all because of lack of communication in the history of the patient's care. Lack of interoperability may be attributed to the absence of a complete and readable patient history.

The EHR and continuity of care record (CCR) can interoperate to make the patient history the focus of all provider-patient discussions and communications. HIPAA Security and the voluntary patient identifier (VPI) can be the impetus for a paradigm shift to accept the EHR as best practice.

Integrating EHR, CCR and emerging technologies

A supermarket has more of the information it needs to readily process groceries at the checkout than a doctor has to take care of an illness in the exam room. Disparate and non-interoperative medical records have no standards and no universal unique personnel identifier. What's wrong with this picture?

According to The Leapfrog Group, almost all clinicians agree that if they have timely access to a patient's complete (lifetime) EHR, then that person's health maintenance, diagnosis and treatment, can be more efficient and less costly. An EHR can reduce the number of tests, provide past history for analysis of a current problem, and improve patient safety. Less interventions, faster diagnosis and beginning of treatment, and better maintenance, mean improved quality of lifetime care. Moreover, less medications, fewer tests and fewer trials mean less chance of error, according to Seth Schiesel in an Oct. 21 *New York Times* article, "In the ER, Learning to Love the PC."

An intermediate step to the EHR is called the Continuing Care Record (CCR). As presented by C. Peter Waegemann, CEO of the Medical Records Institute, "…inter-provider interoperability cannot be achieved in the foreseeable future, and one must look for alternatives to achieve interoperability. The goal is simple. Whenever a patient leaves a hospital, or is referred by the primary physician to any specialist, or is transferred from one provider to another, the relevant information should be available to authorized health providers through a continuity of care record."

HIPAA should be a major force toward achieving adoption of the CCR and EHR. If the EHR is required and implemented, then the EHR/CCR would provide the basic foundation for a data repository and decision support resource necessary for acceptance of emerging technologies such as computerized physician order entry (CPOE) and e-communication.

Among government, private organizations and regulators who should be touting the purpose and pursuit of HIPAA and its quest for continuity of care are the Joint Commission on Accreditation of Healthcare Organizations (JACHO), Centers for Medicare and Medicaid Services (CMS), Agency for Healthcare Research and Quality (AHRQ), and The Leapfrog Group.

Defining emerging technologies

At the ninth Annual HIPAA Summit, I stated that HIPAA will provide the inertia to implement emerging technologies, such as CPOE, EHR and e-communication. One attendee pointed out that CPOE, e-communication and EHR are "not emerging technologies."

My response to this comment was that until health care entities recognize CPOE and EHR as best practices, they are indeed "emerging technologies." If you define CPOE and EHR as new discoveries then the attendee was right. If you define them as technologies beginning to gain rapid acceptance in many providers then these technologies are "emerging." HIPAA needs to be part of the "emerging technologies" and needs to be embraced by covered entities. If health care entities truly believe these technologies are best practices, then why are only a small percentage implemented? Should health care professionals be embarrassed that proven technologies exist, but are rarely used?

A Nov. 2003 study by the Massachusetts Technology Collaborative, "Advanced Technologies to Lower Healthcare Costs and Improve Quality," cited the barriers to emerging technology implementation. More important, the study offered solutions to the barriers. And behind all these solutions, is my strong sense that if covered entities embraced the HIPAA Security standards of confidentiality, integrity and availability (CIA) for electronic protected health information, then we could proceed with something that represents the universal "pre-natal-to-earth" health record, beginning with the CCR and arriving at the EHR.

The initial thrust for CIA

I offer HIPAA Security as the standard to achieving the CIA so urgently called for by clinicians before they can promote CPOE and EHR as a "must."

According to John Halamka, MD, CIO at CareGroup Health System, in an *Information Week* article from July 8, "Doctors need to be incentized to order to foster the adoption of electronic medical records because it's the insurance companies that get the biggest payback in this." The Collaborative Study, which proposed increasing the percentage of emerging technology installations by sharing the cost-benefit with all involved entities, further enhances Halmaka's point. And HIPAA needs to be accepted and promoted by insurers, employers and providers as the basis for this "best practice."

In November 2003, the HIMSS board of directors approved a resolution to establish a voluntary patient identifier (VPI) to be used across health care provider, health plan and geographic boundaries. This VPI would be used by all Americans who voluntarily recognized the importance of a unique identifier for their quality of care and patient safety. It circumvents the impasse of political groups who forget to ask, "Is the EHR good for the patient?"

All too often a political organization's self-interests get in the way of what's good for the patient. I like to ask, "Is this good for the patient?" Let's get more personal. If you were ill, would you not want the provider taking care of you to have access to your current and complete health history?

Changing the culture

Newspapers, magazines, professional journals, and political debates talk about patient safety. The Institute of Medicine's study estimated that more than 55 percent of the deaths in the United States were preventable if CPOE and the EHR had been implemented as best practices. Yet covered entities have not done enough to address preventable deaths. Less than 5 percent of health care facilities use CPOE, and less than 10 percent use an EHR. We've seen progress with e-prescribing mandates, but we had the capabilities to move forward 10 years ago. What would the public response be if a car manufacturer published statistics saying there are 98,000 preventable automobile deaths a year? In fact, there are more preventable inpatient deaths a year than there are car deaths. What a shame. Why haven't consumers revolted?

My graduate health information systems students typically confront me with the barrier that, "hundreds of entities cannot afford computers." My response? "Then let's wait until we are 100 percent computerized before we begin to do something about the 98,000 preventable deaths." Certainly, President Bush's priority to make EHR available to most Americans in the next 10 years is welcome and positive. The tragedy is that in 10 years another million Americans may die because of preventable medical errors.

You have to go back to 1965 with the passage of the Medicare Act to find a health care bill that was enacted for the benefit of consumers. Not until 1996, with the passage of HIPAA, was health care legislation focused on consumers' issues and the concern for security of their medical records and subsequently the consumer empowerment through HIPAA, according to "Leveraging HIPAA to Support Consumer Empowerment" (Journal of Healthcare Information Management, Vol. 14, No. 4). The HIPAA simplification provisions were established in anticipation of emerging technologies. HIPAA was supposed to be the platform from which the amazing use of computers would both improve quality of care and get a handle on costs. So what can health care organizations do to get on the right track?

What next?

The health care industry needs to develop a model of benefit realization and cost-sharing among all stakeholders. This model must have two tenets: (1) The VPI must come from a central repository, as proposed by HIMSS, and (2) HIPAA security standards must provide the CIA of protected health information (PHI). Given these two tenets, which provide for the future "virtual EHR" link among disparate communities, consider the following:

1. We need to proceed on a small community scale to remove the delays caused by political influence. We must form a task force of visionary stakeholders. This group should include community hospitals, physicians, employers, insurers, administrators/technologists, and consumers. (Alternatively, the task force could come from professional trade organizations such as HIMSS, AHIMA, ACHE, Chambers of Commerce, MGMA, state medical associations and HFMA.)

The task force should proselytize and mandate HIPAA CIA and VPI;

- use HIPAA CIA and VPI to agree upon software and technology standards;
- select a "best practice" technology that all will agree to;
- set obtainable milestones and goals and rewards; and, finally,
- publicize, publicize, publicize.

HIPAA sets the security standards necessary for consumer acceptance of personal electronic health information. Keep in mind the following points:

- PHI must be kept confidential and seen only by those "with a need to know."
- PHI maintains its integrity because it has been encrypted and is auditable through a record of who accessed it
- PHI is available immediately to all covered entities. PHI integrity can be enhanced further by verifying PHI upon entry into the EHR (e.g., accepting only lab results within logical test value ranges and medications pertinent to diagnosis).
- A VPI can be the initial personal identifier needed to link disparate EHRs. As HIMSS suggested, VPI would provide time for those Americans who do not yet buy into the CIA of HIPAA Security.

Health care should incorporate the principles of HIPAA Security CIA as the basic foundation for the EHR to improve patient safety, thereby improving quality of care and lowering costs. The EHR will provide the data necessary for emerging technologies such as CPOE to be required as best practice. The VPI will tie together disparate EMRs. And all this will lead to HIPAA Security being recognized as best practice by covered entities. We then will have "an opportunity for continuum of care."

Mr. Priest teaches graduate courses in health administration at Saint Joseph's College of Maine (Standish, Maine), and at New England College (Henniker, N.H.). He recently taught a 30-hour, two-week course on HIPAA Security. He can be reached at www.professorsteve.com and steve@professorsteve.com