Healthcare IT News

Published in partnership with HIMSS

THE NEWS SOURCE FOR HEALTHCARE INFORMATION TECHNOLOGY

HIPAA – An Opportunity for Continuum of Care

by

Stephen L. Priest, FHIMSS, CPHIMS

The Embarrassment

Healthcare entities and their associates should be embarrassed!

Why are healthcare providers not wholeheartedly supporting HIPAA Security? HIPAA should be loudly proclaimed from the treetops as an opportunity to make real the promise of continuity of care.

Most Americans believe their health records are shared among their healthcare providers. The caveat to this is that there is a need to protect the confidentiality and security of each individual's health information. Moreover, clinicians are skeptical in giving up the paper record for concern the electronic health record (EHR) might not be readily available. In effect, there is an on-going dilemma between consumers with their concern for confidentiality and security of their health information, and between clinicians with their concern for the availability of the EHR.

HIPAA – a Major Impetus to Achieving EHR

HIPAA should be a major force to achieving the EHR. The EHR provides the basic foundation for a data repository and decision support resource necessary for technologies such as Computerized Practioner Order Entry (CPOE) and e-communication.

In his Escape Fire –Lessons for the Future of Healthcare[1], Don Berwick readily articulates that although we certainly need for patients and providers to talk one-on-one, that just is not getting the communication necessary to eliminate the estimated 98,000 annual preventable inpatient deaths identified in the Institute of Medicine[2] study, To Err is Human. Clinicians are not doing a good job communicating patient information with each other. They certainly talk to the patient, but "their piece of the pie" is not effectively integrated into the whole patient picture.

When multiple clinicians are involved in the care of a patient, such as physician specialists, pharmacists, nurses, therapists, and dieticians, 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, and then as others are brought into the case, there is a repeat of the drug - and reaction – all because of lack of communication in the history of this patient's care. This scenario happens when there is no complete and easily accessible patient history.

---

[1] www.ihi.org/IHI/Products/Books/EscapeFireDesignsforthe+FutureofHealthCare.htm
[2] www.iom.edu "To Err is Human: Building a Safer Health System", November 1999

A supermarket has more of the information it needs to process groceries at the checkout register more often than a doctor has to take care of 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?

HIPAA and Best Practice Technologies

The banking industry established the paradigm shift of unique identifiers and security provisions years ago with the ATM card. You can go anywhere and access your banking accounts and review your information. The information is secure and protected. Yes there is the occasional highly publicized identity fraud case but the system has adapted to that.

A study[3] by the Massachusetts Technology Collaborative cited the barriers to healthcare's technology implementation for EHR and CPOE. More so, the Collaborative offered solutions to the barriers. And behind all these solutions, although not said by the Study, is my strong sense that if covered entities embraced the HIPAA Security standards of confidentiality, integrity and availability (CIA) for electronic protected health information (PHI), then we can proceed with universal implementation of the EHR.

Let's get personal. If you were ill, would you not want the provider taking care of you to have your current and complete health history available to them?

HIPAA sets the security standards necessary for consumer and clinician acceptance of PHI. PHI is kept **confidential** and seen only by those "with a need to know". PHI has **integrity** maintained because it has been encrypted and is auditable through a record of who accessed it. Verifying PHI upon entry into the EHR can further enhance PHI integrity, such as EHR accepting only lab results within logical test value ranges and medications pertinent to diagnosis. PHI is **available** immediately to all covered entities.

HIPAA Security must be accepted as a basic foundation for the EHR. HIPAA's CIA makes the EHR "best practice". The EHR will provide the data necessary for technologies such as CPOE to be required as "best practice". All this comes because HIPAA Security is "best practice".

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

---

[3] Advanced Technologies to Lower Healthcare Costs and Improve Quality, November 2003, http://www.masstech.org/STATFinal9_24.pdf