PUBLICATION

Health IT: Is It Safe to Exchange Data Yet?

October 29, 2007

It is tempting to believe that the United States has made little progress in the critical area of protecting the privacy and security of electronic health information. But important work has been done and is now available to inform a policy discussion about privacy and security issues in health care. This paper will provide a brief overview of a major nationwide initiative with examples of findings and recommendations.

In the last year, 33 states[1] and Puerto Rico have proposed solutions and implementation plans to address the confusing and conflicting privacy and security requirements they identified. Another initiative will build upon these state efforts, as described below. All of this is designed to provide the guidance and resources needed to build and run secure and trusted health data exchanges.

One important lesson from the process: Privacy and security issues must be addressed whether or not health information is exchanged electronically or on paper. The work revealed significant problems in current paper-based environments, and moving to electronic data exchange—combined with the significant trustbuilding work that is required to do so—can mitigate many of those problems.

Although privacy policy (when should consent be required?) and security standards (how do we protect data?) are intertwined, they are two different things. A decision about privacy policy is best made by a data exchange community so that it reflects local or regional interests, while robust security standards must be adopted nationally and even internationally, so that there is an assurance of security against breaches and the ability to enforce privacy decisions even when data are sent to a distant user.