I wish to comment on the Privacy and Security of information contained in, and exchanged between, EHRs. In addition to the automatic encryption in databases of such information, and its automatic decryption upon viewing, in-transit encryption should always be applied to safeguard data as it is being transmitted over Local Area Networks in clinical settings, as well as to safeguard transmission over the Internet.

Encryption methods such Advanced Encryption Standard (AES) should be employed with key lengths appropriate for the privacy level needed, e.g. perhaps 256-bit or 512 bit. Also, secure key exchange methods should be employed, such as using Elliptical Curve Diffie-Hellman (ECDH).

ECDH uses a math formula to derive the encryption key, and then a public value is calculated and exchanged between the sender and the receiver. The receiver then uses a math formula to derive the symmetric decryption key from the publicly exchanged value. The encryption key value is never itself transmitted, and cannot be computed from the values exchanged, by any unauthorized third party who may have access to data that is exchanged.

The application of such encryption and decryption methods would be fully automated at both the sender and receiver locations, by the software that performed the transmissions. And additional security would be provided by making the keys Ephemeral, that is by only using any given key one time. The keys themselves would be randomly selected from an agreed upon Elliptical Curve.

Actual working examples of ECDHE (Elliptical Curve Diffie Hellman Ephemeral) key exchanges can be seen and tried at www.web2ria.com/#95.

Phil Pearl