TECH TALK

The future of encryption

BY ALEX FLAXMAN, MD, MSE, *BETH ISRAEL MEDICAL CENTER/ALBERT EINSTEIN COLLEGE OF MEDICINE, NY - EMRA TECHNOLOGY COORDINATOR*

The last article discussed patient-physician e-mailing and touched on HIPPA regulations concerning encryption. But does one have to encrypt records?

As Dr. George Krucik, a practicing physician working in the software development industry for over 15 years, said in the last issue, "No." And he's right, there's no requirement to encrypt anything in medicine, especially now that encryption can make technology prohibitive to implement. Since HIPPA seems to grow unfettered by reason, cost, or practicality (try to get an old EKG from another hospital for a patient with EKG changes in your ED for the first time), encryption is sure to become a de facto requirement, if not an out-and-out one.

Even without changes in HIPPA, there may be an advantage to encrypting things now. According to Steve Kalman, a lawyer and expert in computer security law, "encryption works out to the rough equivalent of a HIPPA 'get-out-of-jail-free card.' If you lose Personally Identifiable Information, then you're in for fines when you report it. And you must report it, because if you don't, the fines turn into jail sentences." If the data is encrypted, you're protected because no one else can identify what the content is, let alone read it.

Or, perhaps we should encrypt because patients expect it. Patients trust doctors to keep their private information, well, private. Interestingly, patients can request or be indifferent to encryption based on how you pose the question. If you ask a patient if they would like their records encrypted with the same protection banks or eBay take with their online transactions, they would say yes. On the other hand, if you ask a patient if they expected you to write their handwritten charts with unintelligible symbols only you can decipher, they would undoubtedly say no.

"Patients trust doctors to keep their private information private."

Of course, the most important reason is that we believe, even if not required, encryption is better for patients. That something is better for patients has been enough to drive care in the past (sometimes even in the presence of contradictory evidence) let alone influence a charting methodology.

So, what should we encrypt? "The chart" is a straightforward reply. But what about an email reply to a patient inquiry? Is it sufficient to encrypt the message? How would the patient know we answered the question? After all, a hacker could have intercepted the email and replied to the patient that the proper way to do CPR is to blow in the ear and pump on the big toe. The answer comes in digital signatures and public/private key encryption, something I will discuss in the next article.

In summary, encryption is not required, but it provides a warm fuzzy feeling of security, along with some protections from the financial and criminal threats of HIPPA. It's not that hard to provide currently, and it will undoubtedly get easier as service providers, such as Dr. Krucik, provide products with encryption seamlessly integrated. As for what encryption is, or how to encrypt it, check out this page in the next issue. ■

COMMITTEE APPLICATIONS DUE MARCH 1

EMRA is now accepting applications for its committees:

- Critical Care
- International EM
- Web Site

Members will serve a one-year term beginning April 1, 2005. If you are interested in serving on one of these committees, submit a letter of interest and your CV to pshirey@emra.org. For more information, and complete application instructions, visit www.emra.org and click on "How to Get Involved" under "Interesting Stuff."