

Email encryption for a clean bill of health

Leslie Guy Buckalew, vice president for sales & marketing,
WebLOQ March 31, 2009



Health care organizations have the unenviable role of managing and processing a mountain of patient data. This entails a combination of managing fax-based communications, paper-based office processes, and melding a myriad of different patient record systems and file types. Though Washington is busy touting an overhaul of health care's record keeping, many health care organizations are independently making strides to “digitize” their operations and reduce their reliance on paper -- and the couriering and mailing of medical records -- in an effort to increase efficiency, accuracy and reduce costs.

Emailing records between doctors, health care providers and claims processors has been a first step towards greater efficiencies for a large segment of the medical industry. HIPAA prohibits email communications unless it is encrypted. Though it is part of the day-to-day operations for most organizations, health care providers and medical facilities are beginning to recognize that though email is convenient, the content of their email exchanges (i.e., about patients and our personal information) leaves patients vulnerable to cybercrimes and ID theft. In addition to HIPAA legislation that looks to protect patients, state governments are also beginning to impose new regulations that stipulate data transmission standards and limitations for electronic records exchange.

For instance, in Massachusetts personal information is now defined as a document containing a first name and last name or first initial and last name in combination with one or more of the following data elements that relate to the individual:

- Social Security number;
- Driver's license or state identification card number; or
- Financial account number or credit or debit card number.

The rules are targeted at all companies that handle the personal data of Massachusetts residents, whether they're based in the state or not.

Though the largest health care organizations are able to address concerns of possible security and compliance breaches through expensive, elaborate and secure private networks, the smaller and mid-size organizations are often left to fend for themselves. The industry needs solutions that won't drain IT budgets, entail elaborate training, and constrain smaller organizations from working with health care providers, partners, administrators, and claims processors because of security inconsistencies or incompatibilities.

The entire premise of “digitizing” health care is to improve the system's efficiency, increase accuracy, provide information accessibility and ensure accountability for patient/provider/payor interactions, treatments and payments. What we don't need is a system that makes things overly complex or cost-prohibitive. Health care providers can realize additional cost savings by eliminating the capital expense of equipment such as fax machines and decreased time needed to send and receive critical patient orders and information. A number of email encryption solutions provide the first step towards securing patient data.

As the means of electronic communications become more pervasive, the threat of personal and confidential data getting into the wrong hands also rises. The trend toward requiring the medical industry to enforce secure patient data transfer is mounting. The cost of such solutions must be minimal, the flexibility to integrate with existing architectures will be essential, and the convenience and familiarization of the applications will be critical to their success and use.