Alternative Technologies

Enterprise Integrity: HIPAA

Vol. 6, No. 2

Our industry hears (and talks) a lot about HIPAA. "HIPAA" is jargon for Public Law 104-191, the Health Insurance Portability and Accountability Act passed by Congress on August 31, 1996, a complicated act with various requirements, phases of implementation, and even standards requirements. Many articles point to the requirements imposed by HIPAA as a driver for various software markets, including EAI and BPM. Vendors claim to offer "HIPAA solutions." Unfortunately, HIPAA requirements are rarely explained and it is unclear just exactly which requirements of HIPAA are the "market drivers" or which of those requirements are being addressed by a particular product. Since this month is our health care industry issue, I decided to provide a little more insight into HIPAA. It doesn't take much familiarity with HIPAA to see what is afoot.

HIPAA requires the Department of Health and Human Services (DHHS) to adopt national uniform standards for the electronic transmission of certain health related information, both within and between covered entities. Those entities are required to use those standards for electronic transmission of administrative and financial data under certain defined circumstances. Usage includes both sending and acceptance of specific transactions in the required format and coding. Violators of HIPAA provision face a fine and possible imprisonment.

Ostensibly, the primary motivation behind HIPAA is to reduce costs (about 26% is unnecessary processing overhead) and improve the efficiency of health care related information processing. For example, a study done at the time the law was enacted showed that over 400 proprietary formats were in use in the United States for health claims. Those of us familiar with application integration and supply chain integration know the costs such disparity implies. We also know that "proprietary" is a code word for "independently modifiable," and so for potentially high maintenance costs of the integration solution.

HIPAA exempts paper transmissions and person-to-computer capture (e.g., voice recognition, faxback, and HTML forms) to the extent that the content is equivalent to the corresponding standardized electronic transaction. Initially, only eight types of transactions are standardized: health claims or equivalent encounter information, payment and remittance advice, benefit

coordination, claim status, plan enrollment/disenrollment, plan eligibility, plan premium payments, and referral certification/authorization. In addition, the code sets used to encode these transactions regarding medical diagnosis, procedures, and clinical tests are also standardized.

HIPAA also addresses patient health record portability and confidentiality issues which should result in more consistent health care irrespective of provider. Various identifiers used in the administration of health care to identify health care providers, health plans, employers, products, and patients are to be standardized nationwide. Security standards must be developed and adopted for all health plans, clearinghouses, and providers to follow at all stages of health care information transmission and storage. These security standards apply to storage and before, during and after electronic transmission. HIPAA privacy standards must define both appropriate and inappropriate disclosures of "individually identifiable" health information to protect patient rights.

HIPAA applies to a surprisingly broad range of entities and their contractors, despite being limited to certain health care providers, health care clearing houses, and health plans. For example, "health care provider" includes not only hospitals, but pharmacies and many physicians. Similarly, data entry outsource providers to health care providers, health care clearinghouses, and health plans are generally required to comply with the standards. Obviously, if all entities use the same codes, formats, and security procedures, the health care "supply chain" integration should be straightforward.

Nonetheless, some "gotchas" will perpetuate complexity and plague HIPAA. First, existing paper mediated processes are not directly affected, and some interfacing processes and entities appear to be exempted. Integration problems will persist at the interface points, propagating uncontrolled errors into the system. Second, HIPAA standards are expected to undergo revision and extension over time, and must address new technologies. Although the ability to adapt and change is both positive and necessary, costs of transitioning to new formats and codes will never disappear. Third, penalties for HIPAA violations are not sufficiently prohibitive. For example, the fine for disclosing confidential patient information for commercial purposes is at most $250,000. In today's Internet-mediated business world, potential profits can easily reduce the risk imposed by such fines to nothing more than the cost of doing business.

Given these problems, the IT industry must actively contribute to the long-term success of HIPAA and related agendas like the National Healthcare Information Infrastructure. Beyond costs, our health is at stake. It's about time that healthcare *enterprise* software improved doctor-patient *integrity*.