Creating a Potemkin Village:
HIPAA ‘Quick Fix’ Is Just an Illusion

In the late 18th century, Prince Grigory Potemkin, the most powerful man in Russia — under the reign of Catherine the Great — was employed with the responsibility of colonizing and rebuilding the extremely impoverished Ukrainian region. As legend tells, he was quite an astute politician (wasteful and shameless). After a few years, Catherine, who was also Potemkin’s lover, decided to tour the Ukraine to see how the region had progressed. Potemkin, knowing he had done little to improve the region and not wanting to disappoint Catherine, had come up with an elaborate scheme of illusion. Prior to the Empress’ tour, Potemkin had assembled a team of builders to construct a number of mobile villages to be viewed from Catherine’s barge. As soon as the barge passed out of sight, the make-believe villagers changed out of their costumes, dismantled the village facades, and rebuilt them overnight further downstream. Although this story is mostly fable, the Potemkin Village serves as a poignant metaphor for programs that lack substance and are fraught with disinformation and disillusion.

IT leaders who plan to address the HIPAA regulations and requirements with quick-fix technological solutions will be creating an illusion similar to the Potemkin Village. Organizations must balance technology with good policy to achieve compliance. The challenging HIPAA issues cannot be solved with a veneer of firewalls, single-sign-on products, and digital certificates. The satisfaction one experiences popping each cell on a sheet of bubble-wrapping after the new PC and software have been loaded — waiting for the first Windows screen to appear — is not a pleasure the HIPAA compliance manager will ever know. No quick fix or easy answers will be available. Serious work is required.

As with Y2K, fame will be the result of failure, not success. A job well done will be met with tepid congratulations and possibly generate some skepticism as to the validity of the required effort and expense. The HIPAA-compliant organization will be recognized by the behavior of its members. Unfortunately, behavioral change is not something that you can touch, see, or measure with any degree of precision. It is, however, the primary aspect that one must pursue in order to achieve HIPAA compliance.

The real challenge of HIPAA compliance lies in how an organization can harness its knowledge to support superior patient care, promote this knowledge to all who participate in this endeavor, and keep this knowledge away from those who would use it maliciously. True compliance will require that each member of the organization develop a tacit understanding of what information is private and what information can be shared without restraint. To achieve this level of inherent organizational behavior, a comprehensive educational effort must begin at the highest levels within the organization. Decisions as to who can access information must be uniform, consistent with each role, and decentralized. The responsibility for authorizing access cannot be centrally controlled. Even though most organizations will initially attempt to centralize this process, security administration will soon become too cumbersome to manage once the entire organization’s access is closely scrutinized under HIPAA.
Furthermore, who is in a better position to decide who can request reports or computer access than the person responsible for each specific business unit? Security staff and other personnel, charged with handling sensitive information, must be officially screened. Although thorough background checks can be expensive and time consuming, the HIPAA-compliant organization must be able to demonstrate that these employees have a clean background and ethical character. Additionally, those who breach security and confidentiality must be punished. To truly secure information from abuse, the organization must define a clear policy for proper use, develop a routine and reliable auditing process, and enforce this policy with sanctions up to and including termination of employment or contractual agreement for business partners who commit violations.

Safeguarding the main computer facility should also be given top priority. After years of rigorous financial audits, most IT leaders already have a comprehensive disaster recovery plan in place. Inspection of this plan will usually yield extensive backup procedures with offsite media storage, hot or cold site facility restoration arrangements, emergency power continuation, temperature control contingencies, and environmental disaster protection for fire and floods. The most important feature of the contingency plan — operational and business unit downtime procedure — is often given lip service. When is the last time you intentionally pulled the plug on the computer room? As we continue on a path of complete clinical automation, failure and patient harm are imminent if we cannot provide safe patient care during a temporary disruption of the network or computer facility. In a fully automated environment, competence in “manual” patient care requires regular practice.

The more unfamiliar humans are with a process, the more prone they are towards error. Although downtime, scheduled or unscheduled, can be a harrowing experience for both users and the IT staff, organizations that do not regularly test their operational efficiency under offline conditions will never be HIPAA compliant.

Finally, HIPAA policies and procedures must blend with existing operational protocol so that reaching and maintaining compliance ceases to be a major draining focus and initiative. The astute HIPAA compliance manager should strategically plan his or her own obsolescence. The multidisciplinary steering committees, executive sponsors, HIPAA project managers, program management offices, and advisory teams should one day dissolve just as their Y2K counterparts did. Unlike the millennium rollover, preparation for HIPAA should yield a new philosophy at all levels of the organization. No longer can wind-blown lab reports dance across the visitors’ parking lot. Confrontations with patients and physicians, as well as consultations between caregivers will take place only at the bedside, exam room, behind closed doors, or by other intruder-proof means. Release of medical information will require just cause, patient consent, and audibility throughout each step. Caretakers of information will be fully accountable from a legal, ethical, and moral perspective. Only when an organization can achieve this level of natural human conduct will new technology achieve its intended objective and create more than an illusion of security as in a Potemkin Village.

As editor of the Spring 2002 issue of the Journal of Healthcare Information Management, I am happy to present to you this collection of special interest columns and articles focusing on another very important issue — HIPAA. In this edition, there are a number of examples, strategies, opinions, and success stories that will be useful for those who are helping their organizations achieve HIPAA compliance. Articles in the areas of organizational readiness and collaboration, the use of software-aided benchmarking, HIPAA practice comparisons, and other HIPAA program case studies provide a broad and diverse overview of many compliance and progress measurement techniques. In addition, special interest columns and articles offer the reader some interesting “intermezzi” that add a cross-section of valuable information in the areas of Integrating the Healthcare Enterprise (IHE), HIPAA Leadership, ROI strategy, Telemedicine, and other original contributions. Furthermore, another addition of “Ask Mr. H.I.T.man” continues to be a HIMSS favorite, providing expert advice on “hot” topics with a healthy dose of humor. Authors, I thank you.

Finally, I would like to thank all of the professional staff at HIMSS, the peer reviewers, and the HIMSS editorial review board. Your contribution will help HIMSS professionals tackle the many challenges in achieving HIPAA compliance. As we evolve as an industry, we will continue to address the concerns of the healthcare public with a combination of policy, strategy, and technology. The more we share our experiences with each other, the faster we will achieve these goals. My hopes are that JHIM continues to be an important contribution to this process by giving each member a valid, reliable, and useful source of information.

RICHARD. D. LANG, EDD
EDITOR, JOURNAL OF HEALTHCARE INFORMATION MANAGEMENT
AND PRINCIPAL, KNOW-POWER, LLC
GLENSIDE, PENNSYLVANIA