Commentary

You Can Still Meet the HIPAA Privacy Deadline

A healthcare delivery organization, or a midsize health plan or clearinghouse, can meet the minimum requirements of the HIPAA privacy regulation by following these guidelines, even if it has done little or nothing to date.

You Can Still Do It!

The deadline for mandatory compliance with the U.S. Department of Health and Human Services' Health Insurance Portability and Accountability Act (HIPAA) privacy regulation is 14 April 2003. As of February 2003, it is still possible for most single-entity healthcare organizations (HCOs) to comply with the minimum requirements of the HIPAA privacy regulation by using an accelerated internal program, even if dedicated funding is minimal or nonexistent. This will not be easy — an accelerated compliance program will stress an organization. However, with highly visible executive support, as well as a pragmatic, prioritized approach and the right project leader, a minimal compliance posture can be achieved, the risk of adverse publicity can be reduced, and a framework can be implemented for ongoing improvements in the protection of individual privacy.

Gartner's research into the state of the healthcare industry's HIPAA compliance efforts indicates that most healthcare provider and payer organizations will be largely, if not fully, compliant with the privacy regulation by the deadline (see "HIPAA in the Homestretch: An Industry Progress Report"). Covered entities that do nothing, or that leave obvious gaps in compliance with patient-facing requirements, likely will suffer significant damage to their reputations in their local communities.

The Regulation Is Not That Complex

The privacy regulation is not nearly as complex and onerous as the debate regarding its adoption might lead some to believe. It affirms some patients' rights that most HCOs have always honored. It places some restrictions on the use or disclosure of a patient's protected health information (PHI) for purposes other than treatment, payment and healthcare operations (TPO). It also imposes some new, minor record-keeping responsibilities on HCOs to track external disclosures of PHI for some restricted purposes. Most covered entities should be able to comply with the HIPAA privacy regulation without investing in additional hardware or software.
There are only a few patient- and member-facing procedures and forms that must be in place on 14 April 2003. A covered entity must designate a privacy officer, and the entity must provide patients/members with a written notice of its privacy practices. The notice must include a description of how patients can request copies of their healthcare information, and how they can challenge the accuracy of this information. It must also describe how patients can request an accounting of certain external disclosures of their PHI.

Although no aspect of the HIPAA privacy regulation can or should be ignored, it is sensible to prioritize compliance efforts on those provisions that require visible evidence of compliance on 14 April 2003. In most cases, covered entities have up to 60 days to produce copies of requested patient health information and records of external disclosures. In a worst-case scenario, this amounts to a deadline extension to finalize the procedures that implement these privacy policies.

There Are Excellent Self-Help Resources Available

The HIPAA privacy regulation requires covered entities to have written privacy policies, and to develop a set of notices, forms and business associate agreements. Fortunately, there are several free or low-cost sources for sample documents in electronic form, which easily can be adapted to most HCOs' situations. For example, the Atlantic Information Services' (AIS') "HIPAA Patient Privacy Compliance Guide" ($417) consolidates basic information and provides sufficiently detailed recommendations to enable an HCO to organize and manage an accelerated HIPAA privacy regulation compliance effort. For an additional $305, HCOs can purchase a companion CD-ROM, prepared by Strategic Management Services, that contains a comprehensive set of policy templates and sample documents that appear in the AIS guide (see "AIS' Road Map for Privacy Procrastinators").

There is no time left for HCOs to review and compare alternative sources of basic information. Therefore, Gartner recommends that HCOs that are undertaking an accelerated HIPAA privacy compliance program to meet the 14 April 2003 deadline, without the budget to bring in external consulting help, immediately purchase the AIS HIPAA Patient Privacy Guide with the CD-ROM companion.

More Good News

Most provider organizations will find that their health information management (medical records) departments have provided patients with copies of their medical records, and dealt with disputes over these records' contents, since the organizations' first day of business. There likely will be one or more correspondence clerks whose role includes screening external requests for copies of patient medical records, assembling the records to satisfy legitimate requests, and maintaining a log of all records released (for whatever reason). This is a firm foundation on which to build a HIPAA privacy compliance strategy.

You Need High-Level, High-Energy Leadership

Highly visible, enthusiastic, executive-level sponsorship is a necessary, but not sufficient, condition for the success of an accelerated HIPAA privacy compliance program. The project also will need a well-respected, richly networked, operational business leader who shares the pragmatic approach espoused in this research to provide day-to-day leadership. Finally, the project leader must pick a small team to work closely with him or her to energize the organization and get the work done by the deadline. "Organizing for Accelerated HIPAA Privacy Compliance" provides guidelines on building a "lean, mean" privacy implementation team.
You Must Have a Pragmatic Approach

An accelerated compliance effort must take a ruthlessly pragmatic approach to succeed. The motto of an accelerated HIPAA privacy compliance project should be "a reasonable response with available resources."

Compliance is primarily about implementing policies and procedures. Initially, the procedures do not have to be optimal. Think of the project as defining required policies, educating employees about the policies as appropriate and, if necessary, implementing "place holder" procedures, while planning for the continuous improvement of procedures in response to how patients and members actually exercise their rights under the regulation.

Assigning Tasks and Tracking Progress

Compliance tasks will need to be quickly identified from the regulation and assigned to work groups. There are many tools available that can assist with this process. However, most come bundled with consulting services, for which HCOs faced with accelerated privacy compliance programs likely will not have funds. There certainly will be no time to conduct a traditional selection process. Therefore, unless someone on the core implementation team has familiarity with, and immediate access to, a proven, low-cost or no-cost alternative, Gartner recommends that small to midsize provider and payer organizations purchase and use the North Carolina Healthcare Information and Communications Alliance's HIPAA EarlyView Privacy gap assessment and compliance checklist tool (see "HIPAA EarlyView Privacy: A Valuable Self-Assessment Tool") or Xpediate Consulting's Xpediator (see "Xpediator: A Self-Administered HIPAA Assessment Tool").

Training Is Key

Employee training will be the most difficult of the HIPAA privacy regulation's requirements to meet in an accelerated mode. Training, as necessary and appropriate for individual employees to carry out their jobs, is required for the entire workforce on the HCOs' HIPAA-compliant privacy policies and procedures. Thus, training cannot begin until the requisite policies and procedures have been developed. In this area, some money will have to be spent if HCOs expect to meet the deadline from a cold start now.

Gartner recommends a Web-browser-delivered, computer-based training (CBT) program for HIPAA privacy training of an HCO's workforce when time is of the essence. HCOs should check with their principal application vendors first, because they may have CBT products for HIPAA privacy, or they may be able to connect HCOs with third-party partners that have these products. Vendors that offer CBT products for HIPAA privacy training include:

- Acclaim Services (www.acclaimtraining.com)
- Covansys (marketing.covansys.com/papers_intro.asp)
- Eclipsys (www.eclipsys.com/solutions/services.asp)
- EduNeering (www.eduneering.com/solutions_overview.asp)
- Health Care Compliance Strategies (www.hccs.com)
- HCPro (www.hcpro.com/content.cfm?content_id=25404)
Bottom Line: Healthcare organizations that have done little to address the HIPAA privacy regulation still can meet its minimum requirements by the 14 April 2003 deadline by using an accelerated compliance program. Achieving success will require: unequivocal executive sponsorship; a dynamic project leader; a ruthlessly pragmatic approach; and reliance on sample policies, procedures, contracts and forms, which are available from several industry sources at a nominal cost. Even with an accelerated compliance program, tasks will have to be completed after the deadline has passed. Further improvements in privacy-related services will be possible and beneficial to customer relationship management. However, the risk of embarrassment to organizations’ reputations from a real or nominal violation of the HIPAA privacy regulation will be dramatically reduced.