

The Final HIPAA Security Rule Offers More Flexibility

A long-awaited, revised and now final U.S. healthcare regulation increases the flexibility of healthcare organizations to comply. Encrypting Internet e-mail containing protected health information is no longer an absolute requirement.

Event: On 13 February 2003, the Centers for Medicare and Medicaid Services (CMS) announced that the final rule on security will be published in the Federal Register on 20 February 2003 (for a copy of the 289-page rule, see www.cms.hhs.gov/hipaa/hipaa2/default.asp). The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandated the rule. The meat of the regulation is the 16 double-spaced pages between page 264 and page 279 of the above copy. The scope of final rule is substantially the same as the draft released in August 1998. As long predicted by CMS, it deleted the section on electronic signatures.

First Take: CMS has introduced a major new wrinkle in the regulation that dramatically increases the flexibility that covered entities have in responding to its security standards. Each "Implementation Specification" section of the regulation is now labeled as "Required" or "Addressable." A covered entity must implement Required sections as written. However, for Addressable sections, the covered entity can document why the implementation specification is not reasonable or appropriate to its circumstances and implement an equivalent measure, if reasonable and appropriate. In determining the reasonableness and appropriateness of an implementation specification, covered entities may consider (among other criteria) the "cost of security measures" and the "probability and criticality of potential risks to electronic protected health information."

Twenty-two of 42 implementation specifications are Addressable, including all those involving IT security technology. Most notably, the Addressable implementation specifications include "Integrity Controls" and "Encryption" related to the standard for "Transmission Security." At a minimum, this approach will encourage tens of thousands of doctors in individual and small group practices to go ahead with unencrypted e-mail for routine exchanges with their patients such as requests for appointments and prescription renewals. Such communications carry infinitesimal risks and significant benefits. Large healthcare organizations will rethink a forced march to universal encryption. Emphasis will shift from e-mail security to content filtering. The real risk has never been sniffing and intercepting, but authorized users doing things they should not.

The new flexibility should reduce the total cost of compliance for the United States by at least 50 percent.

Analytical Source: Jim Klein, Gartner Research

Recommended Reading and Related Research

Gartner

The content herein is often based on late-breaking events whose sources are believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of the information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The conclusions, projections and recommendations represent Gartner's initial analysis. As a result, our positions are subject to refinements or major changes as Gartner analysts gather more information and perform further analysis. © 2003 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction of this publication in any form without prior written permission is forbidden.

- “HIPAA and the Encryption of Protected Health Information” — Gartner answers questions about the necessity and adequacy of encrypting personal health information to conform to the draft security standards of HIPAA. **By Jim Klein**
- “You Can Still Meet the HIPAA Privacy Deadline” — 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. **By Jim Klein**

(You may need to sign in or be a Gartner client to access all of this content.)