Editors: Martin R. Stytz, mstytz@att.net
Shari Lawrence Pfleeger, pfleeger@rand.org
Chuck Pfleeger, c.pfleeger@computer.org

# BookReviews

## Protecting Consumers' Private Health Information

Scott Forbes
Microsoft

Readers know they're dealing with a sensitive topic when a practical guidebook devotes a half-page to limiting the authors' liability and disclaiming any warranty for the book's subsequent content.

Reviewed in this issue:

Kevin Beaver and Rebecca Herold, *The Practical Guide to HIPAA Privacy and Security Compliance*, Auerbach Publications, 2003, ISBN 0-8493-1953-6, 496 pages, US$79.95.

Luckily for both the authors and readers, *The Practical Guide to HIPAA Privacy and Security Compliance* provides a wealth of information that should help companies comply with the myriad requirements found in the US Health Insurance Portability and Accountability Act of 1996. HIPAA, which contains privacy and security requirements designed to help protect consumers' private health information (PHI) such as medical records, applies to most of the healthcare industry as well as business associates disclosing PHI on behalf of healthcare companies.

The book is designed for those responsible for HIPAA-compliance activities that need less legal and political background, but more practical explanations and commonsense implementation guidance.

The book's main strength is its abundant and varied content. It thoroughly describes the main provisions of HIPAA's security and privacy requirements using actual language from the legislation interspersed with the authors' commentary. This format, in addition to the numerous exhibits, tables, and checklists explaining the sometimes impenetrable HIPAA text and government agency guidelines, helpfully guides readers through the labyrinthine HIPAA requirements. For example, the authors include two detailed, yet clear, decision trees to help businesses determine whether their health plans are covered by HIPAA. Later in that same section—like all sections—a multiple-choice quiz helps readers review the material they have (hopefully) learned.

*Practical Guide*, by virtue of its breadth and depth, can also help companies identify compliance areas that require additional research. In a short, no-nonsense chapter, the authors describe the difficulties in determining whether state law preempts particular HIPAA provisions, offers a brief decision tree for readers concerned about their state laws further, and then provides links to online HIPAA preemption information for more than 40 states.

For example, the glossary's confusing organization makes it difficult to find even common abbreviations such as PHI without hunting through subsections dedicated to particular regulations.

The authors, in some instances, omitted useful practical information in the interest of streamlining their recommendations. In chapter 22, for example, they neglect to mention frontline health workers when discussing the most likely candidates for a Computer Emergency Response Team. These workers—whether emergency room nurses, doctors, or paramedics—are critical to implementing incident-response programs in a real-world environment because they understand their companies' actual organizational structures and daily routines.

Compliance with HIPAA is difficult, time-consuming, expensive, and ongoing. This book helps ease these challenges with its exhaustive treatment of HIPAA's requirements in a friendly, practical manner. Despite the book's size and richness, compliance professionals are likely to feel more energized than overburdened after using this book because it helps answer specific questions in specific contexts without adding unneeded conversational filler. □

*Scott Forbes is the security and privacy compliance manager in Microsoft's Law and Corporate Affairs group. He has a PhD in telecommunications from Pennsylvania State University and is completing his law degree at George Washington University. He is a member of the IEEE, the American Bar Association, and the Information Systems Audit and Control Association (ISACA). Contact him at scottfo@microsoft.com.*