Preface

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule introduced industry-standard information technology security practices to the healthcare field. It provides needed security protections for vital and sensitive health information. The Security Rule, however, poses a challenge for people charged with implementing it, or advising those who must implement it. On one hand, attorneys in the healthcare field may be unfamiliar with information security practices, especially technical security controls. On the other hand, information security professionals may have no formal training in the law.

This book attempts to bridge the gap between the law and information security practices. HIPAA and the Security Rule are sources of law, but the Security Rule also acts as a source of information security practices. The Health Information Technology for Economic and Clinical Health Act, also called the HITECH Act, imposes additional security requirements. This book serves as a reference to a wide audience: healthcare and information security professionals implementing the HIPAA Security Rule and Breach Notification Rule, as well as attorneys and business professionals advising them. It is dedicated to healthcare professionals who struggle every day with meeting their obligations to provide care and services for patients and at the same time are seeking to protect the security of patients’ health information. I hope that this book provides vital guidance and information for those involved in compliance with the Security Rule and Breach Notification Rule.

Chapter 1 serves as an introduction to the topic of HIPAA security and the Security Rule. Chapter 2 discusses the reasons for the enactment of the HIPAA legislation and its mandate to develop regulations, including the Security Rule. It also discusses more recent health information technology initiatives. Chapter 3 clarifies the relationship between HIPAA’s Privacy Rule and Security Rule. Chapter 3 also describes how the HIPAA legislation and the Privacy Rule themselves call for the security of health information. In addition, it discusses the HITECH Act and its requirements. Chapter 4 covers the scope of the HIPAA Security Rule. Specifically, chapter 4 establishes what
information the Security Rule protects and which entities are covered by the Security Rule.

Chapter 5 is the core of this book. Chapter 5 serves as a section-by-section analysis of the HIPAA Security Rule. The section-by-section treatment of the Security Rule is to provide a comprehensive set of guidelines for implementing the Security Rule. Chapter 5 distinguishes between requirements under the law and other so-called “addressable” practices that are not required. A covered entity or business associate must analyze addressable practices in a risk assessment and management process and determine whether they are reasonable and appropriate to implement under its particular circumstances.

Chapter 6 addresses the breach notification requirements for covered entities and business associates. Chapter 7 covers compliance and enforcement. First, it discusses the state of the industry’s implementation of the Security Rule. Second, it describes the enforcement of the Security Rule, including the Department of Health and Human Services Office for Civil Rights investigations, the imposition of civil money penalties, and state attorney general enforcement actions. Chapter 8 reports on private plaintiff litigation arising out of the Security Rule. Chapter 9 focuses on particular newer and emerging technologies. It explains these technologies, as well as their security and resulting HIPAA security issues. I present some conclusions in chapter 10.

The appendices to this book contain useful reference materials. Appendix 1 sets forth the administrative simplification provisions of the HIPAA legislation. Appendix 2 contains HITECH Act provisions that supplement HIPAA security and set the stage for the HIPAA Final Omnibus Rule. Appendix 3 contains general administrative requirements from title 45 of the Code of Federal Regulations, part 160, which includes the regulations concerning enforcement. Finally, Appendix 4 contains the HIPAA Security Rule, Breach Notification Rule, and Privacy Rule.

I received assistance on the first edition of this book and inspiration for my work in the area since the first edition from the Information Security Committee (ISC) and the Healthcare Technology Committee of the ABA Section of Science & Technology Law. The ISC is an interdisciplinary group of lawyers, technologists, and other professionals that explores legal, business, and technical aspects of securing information and critical infrastructures within computer systems and
networks, such as the Internet. The Healthcare Technology Committee explores information technology issues, such as privacy and security, in the healthcare field. If you wish to delve further into HIPAA security, and discuss healthcare security issues with other professionals, I recommend joining these two committees. Both attorneys and nonattorneys are welcome to join.

For attorneys in the Health Law Section, I recommend exploring the eHealth, Privacy & Security Interest Group. This interest group focuses on cutting edge issues dealing with technology, privacy, and security as they relate to health care. Its website includes a number of member benefit resources.

Stephen S. Wu