Even before the HIPAA privacy regulations were finalized on December 28, 2000, HIPAA has been the subject of countless hours of study, analysis, and compliance efforts within the health care industry and beyond. Almost two decades later, and more than 15 years after the first edition of this book, the privacy and security requirements of HIPAA are the subject of significant confusion and uncertainty. Some companies have argued that they are not subject to HIPAA’s requirements, only to find out that they are now subject to state privacy laws that carve out HIPAA, such as the California Consumer Privacy Act and the Florida Information Protection Act, and those who have complied with HIPAA’s requirements have life a bit easier because they are under HIPAA’s protective umbrella.

In the coming years, we expect to see the health care industry and Congress focus even more on data privacy and security. Currently, there is discussion at the federal level to strengthen the privacy rules and create a national privacy law similar to the European Union’s General Data Protection Rule. As the laws and social pressure evolve and tighten the reigns on health care privacy, patients and providers will continue to become more concerned about maintaining the security and privacy of data while rising to the challenge of balancing privacy while promoting patient access and quality care.

In this book, we have attempted to create a useful guide for those who are new to HIPAA as well as provide updates for
seasoned veterans of HIPAA. This book expands on the first edition and includes the Security Rule, the HITECH Act, and the Breach Notification Rule along with extensive discussion about HIPAA’s parameters, practical applications, and lessons learned over the past 15 years. To assist you in complying with HIPAA’s complex requirements, we have included forms and experiential anecdotes that we hope you will find helpful in your ongoing HIPAA compliance efforts.