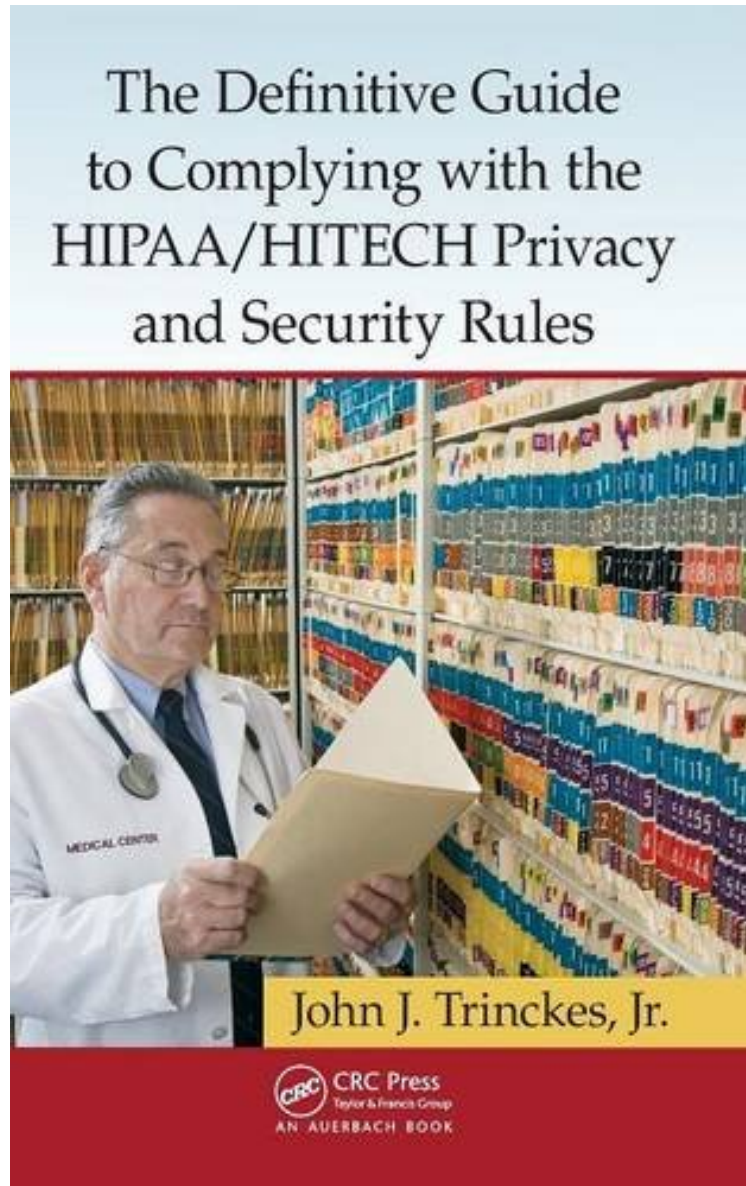


The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules

John J. Trinckes Jr.

*ebooks / Download PDF / *ePub / DOC / audiobook*



DOWNLOAD



READ ONLINE

#1593792 in Books Auerbach Publications 2012-12-03 Original language: English PDF # 1 9.21 x 1.06 x 6.141, .95 #File Name: 1466507675472 pages | File size: 30.Mb

John J. Trinckes Jr. : The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules before purchasing it in order to gage whether or not it would be worth my time, and all praised The Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules:

1 of 3 people found the following review helpful. Beware of So-called Kindle Version
By G. Kuyat
This book is sold as a Kindle version. However, the Kindle version works on none of the e-ink devices. There is a disturbing trend of deprecating perfectly good e-ink products. Neither the android mobile phone, nor my Kindle 2nd generation could view this book. Neither device warns that the book is unreadable. Very disappointing.
5 of 5 people found the following review helpful. Thorough and comprehensive reference guide
By Ben Rothke
I was flattered when John Trinckes asked me to write the forward to *Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules*, given the importance of the topic. There are plenty of books on HIPAA going back a number of years. But there is a dearth of books on HITECH. For the uninitiated, HITECH is the Health Information Technology for Economic and Clinical Health act, which was part of the American Recovery and Reinvestment Act; the stimulus program that President Obama pushed in early 2009. In a nutshell, HITECH takes HIPAA and adds a lot of details, particulars, and perhaps more importantly, enforcement aspects. HIPAA covers the principal areas of administrative, physical and technical controls. The book details the requirements around these areas and shows how covered entities can ensure they are compliant. The book is 400 densely packed pages encompassing 400 pages that provides the reader with a thorough overview of the core elements that they need to know about HIPAA and HITECH. While a completely comprehensive topic on the subject would likely be close to 1,000 pages in length, the book covers all of the core areas around HIPAA and HITECH. Areas covered in the book include an overview of what meaningful use means, details of what the impediments to HIPAA/HITECH compliance are, overview of a HIPAA / HITECH privacy and security audit program, details on breach notification guidelines, and much more. For those looking for a thorough and comprehensive reference guide on the topic, the *Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules* will be a tremendous asset.

The *Definitive Guide to Complying with the HIPAA/HITECH Privacy and Security Rules* is a comprehensive manual to ensuring compliance with the implementation standards of the Privacy and Security Rules of HIPAA and provides recommendations based on other related regulations and industry best practices. The book is designed to assist you in reviewing the accessibility of electronic protected health information (EPHI) to make certain that it is not altered or destroyed in an unauthorized manner, and that it is available as needed only by authorized individuals for authorized use. It can also help those entities that may not be covered by HIPAA regulations but want to assure their customers they are doing their due diligence to protect their personal and private information. Since HIPAA/HITECH rules generally apply to covered entities, business associates, and their subcontractors, these rules may soon become de facto standards for all companies to follow. Even if you aren't required to comply at this time, you may soon fall within the HIPAA/HITECH purview. So, it is best to move your procedures in the right direction now. The book covers administrative, physical, and technical safeguards; organizational requirements; and policies, procedures, and documentation requirements. It provides sample documents and directions on using the policies and procedures to establish proof of compliance. This is critical to help prepare entities for a HIPAA assessment or in the event of an HHS audit. Chief information officers and security officers who master the principles in this book can be confident they have taken the proper steps to protect their clients' information and strengthen their security posture. This can provide a strategic advantage to their organization, demonstrating to clients that they not only care about their health and well-being, but are also vigilant about protecting their clients' privacy.

About the Author
John ("Jay") Trinckes, Jr., CISSP, CISM, CRISC, CEH, NSA-IAM/IEM, MCSE-NT, A+, is the chief information security officer (CISO) for Path Forward IT, a managed service provider of IT and security services for the healthcare industry. Jay has previously worked as a senior information security consultant and authored *The Executive MBA in Information Security*, published by CRC Press in 2009. Trinckes has developed enterprise-level information security management programs for multiple clients and conducted countless successful internal/external vulnerability/penetration assessments and other technical compliance audits. He has been instrumental in developing policies, procedures, audit plans, compliance assessments, business impact analyses, and business continuity and disaster recovery plans for many clients. He also conducts security awareness training and other presentations related to information security. He provides a unique perspective on compliance as a result of his previous work experience as an information security risk analyst, IT manager, system administrator, and law enforcement officer.