1. Record Nr. UNINA9910254851903321

Autore	Thompson Eric C
Titolo	Building a HIPAA-Compliant Cybersecurity Program : Using NIST 800-30 and CSF to Secure Protected Health Information / / by Eric C. Thompson
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2017
ISBN	9781484230602 1484230604
Edizione	[1st ed. 2017.]
Descrizione fisica	1 online resource (XXII, 297 p. 67 illus., 29 illus. in color.)
Disciplina	610.289
Soggetti	Data protection Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Part I: Why Risk Assessment and Analysis -- Chapter 1: Not If, But When -- Chapter 2: Meeting Regulator Expectations -- Chapter 3: Selecting Security Measures -- Part II: Assessing and Analyzing Risk -- Chapter 4: Inventory Your ePHI -- Chapter 5: Who Wants Health Information -- Chapter 6: Weaknesses Waiting to Be Exploited -- Chapter 7: Is It Really This Bad? -- Chapter 8: Increasing Program Maturity -- Chapter 9: Targeted Non-technical Testing -- Chapter 10: Targeted Technical Testing -- Part III: Applying the Results to Everyday Needs -- Chapter 11: Refreshing the Risk Register -- Chapter 12: The Cybersecurity Roadmap -- Part IV: Continuous Improvement -- Chapter 13: Investing for Risk Reduction -- Chapter 14: Third Party-Risk: Beyond the BAA -- Chapter 15: Social Media, BYOD, IOT and Portability -- Chapter 16: Risk Treatment and Management -- Chapter 17: Customizing the Risk Analysis -- Chapter 18: Think Offensively -- Appendix A. NIST CSF Internal Controls -- Appendix B. NIST CSF to HIPAA Crosswalk -- Appendix C: Risk Analysis Templates.- .
Sommario/riassunto	Use this book to learn how to conduct a timely and thorough Risk Analysis and Assessment documenting all risks to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI), which is a key component of the HIPAA Security Rule. The requirement is a focus area for the Department of Health and Human

Services (HHS) Office for Civil Rights (OCR) during breach investigations and compliance audits. This book lays out a plan for healthcare organizations of all types to successfully comply with these requirements and use the output to build upon the cybersecurity program. With the proliferation of cybersecurity breaches, the number of healthcare providers, payers, and business associates investigated by the OCR has risen significantly. It is not unusual for additional penalties to be levied when victims of breaches cannot demonstrate that an enterprise-wide risk assessment exists, comprehensive enough to document all of the risks to ePHI. Why is it that so many covered entities and business associates fail to comply with this fundamental safeguard? Building a HIPAA Compliant Cybersecurity Program cuts through the confusion and ambiguity of regulatory requirements and provides detailed guidance to help readers: Understand and document all known instances where patient data exist Know what regulators want and expect from the risk analysis process Assess and analyze the level of severity that each risk poses to ePHI Focus on the beneficial outcomes of the process: understanding real risks, and optimizing deployment of resources and alignment with business objectives What You'll Learn: Use NIST 800-30 to execute a risk analysis and assessment, which meets the expectations of regulators such as the Office for Civil Rights (OCR) Understand why this is not just a compliance exercise, but a way to take back control of protecting ePHI Leverage the risk analysis process to improve your cybersecurity program Know the value of integrating technical assessments to further define risk management activities Employ an iterative process that continuously assesses the environment to identify improvement opportunities.