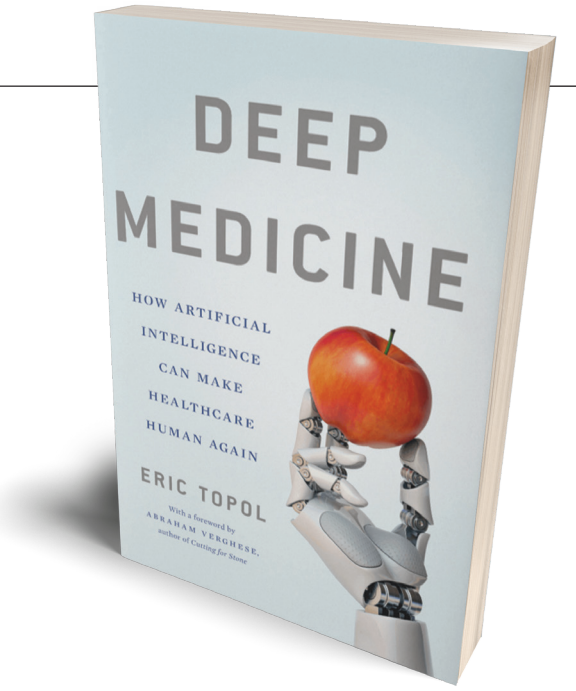
HOW ARTIFICIAL INTELLIGENCE CAN IMPROVE HEALTHCARE

Dr. Eric Topol



Over the years technology has played an indispensable role in advancing medicine and heralded major changes to the healthcare industry. Patients now have access to some of the best diagnostic tools, innovative treatments, and innumerable types of minimally-invasive surgeries, leading to more effective and reliable outcomes.

But in his latest book, Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again, Dr. Eric Topol unpacks the ways in which artificial intelligence (AI) can revolutionize how doctors relate to their patients.

Dr. Topol, a cardiologist and founder of the United States-based Scripps Research Translational Institute, has long been a pioneer in digital health. For decades his ideas have been making waves in the healthcare technology field.

With an excellent understanding of a highly complex issue, Topol offers a thought-provoking and measured idea of the future of medicine.

Published by Basic Books, the 400-page Deep Medicine outlines a vision comprising three main elements and based on an AI-driven strategy that can be harnessed to improve the relationship between doctors and patients for the greater good of healthcare.

The first element involves the gathering of medical, social, behavioral, and family histories ofthe patient, including an analysis of their biology.

The second element involves pattern recognition and machine learning that doctors will use to better diagnose their patients. This method, Topol believes, will facilitate discovery of new medicines and better understanding of complex medical cases.

The third element aims to ensure that AI keeps sight of theessential human component in medicine. The idea is to allow machines to carry out the tasks that are more suitable for automation and to free up doctors and other healthcare professionals to focus on caring for their patients.

Offering a critique of contemporary medicine, Topol suggests that “rather than an emotional connection between patients and doctors...we have an emotional breakdown, with disenchanted patients largely disconnected from burned-out, depressed doctors.”The book also pinpoints how, in a world where internet security is such a crucial issue touching people in their daily lives, reliance on AI in healthcare creates certain vulnerabilities, notably through breaches of privacy security and hacking.

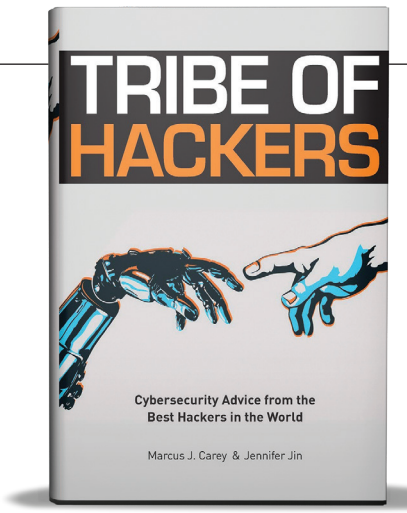
Topol’s book will be interesting to almost anyone interested in healthcare or advanced technology. You don’t need to be a health expert to learn from the book, since Topol’s description of his ideas can easily be grasped by the average reader.

Topol has written an excellent book about AI in healthcare. The personal stories he shares underscore the need for empathy as the vital element of Deep Medicine.

Left:
Dr. Eric Topol

FOR ADVICE ON CYBER-SECURITY, LISTEN TO THE WORLD'S HACKERS

Marcus J. Carey and Jennifer Jin



An imperative for all in this Digital Age is appreciating that our privacy is more exposed than at any other time in our history. Every day we hear truestories about identify theft and online data breaches that directly affect people's lives—often in quite devastating ways. As governments and corporations around the world work assiduously to protect themselves and their workers from digital intrusions by enhancing cyber-security systems, others relentlessly seek to undermine and sabotage those same systems.

It's vital in such an environment that individuals gain a solid grasp of the ways in which they are personally vulnerable in cyber space as this will help them be more mindful of the actions they take while navigating it. Simply put, it is a lot easier to protect yourself from hackers, malware, and viruses if you first familiarize yourself with best practices of cyber-security. That's why Marcus J. Carey and Jennifer Jin have compiled answers to 14 common questions that people ask on cyber-security. Questions such as What is the best book or movie that can be used to illustrate cyber-security challenges? Or do you need a college degree or certification to be a cybersecurity professional? Or What is your favorite hacker movie?

For answers, Carey and Jin reached out to 70 cybersecurity gurus, including Wendy Nather, David Kennedy, Bruce Potter, and Lesley Carhart. This was the genesis of their book Tribe of Hackers, a compilation of industry, career, and personal insights from those professionals. Independently published, the book blends the views of hackers and cybersecurity specialists. By pulling together a diverse group of hackers, Carey and Jin—who hail from quite different professional backgrounds themselves—have done a wonderful job of juxtaposing expert viewpoints. And so you get a variety of perspectives on the same subject, along with universal agreement on some topics.

For instance, Bruce Potter, chief information security officer at cyber-security company Expel, in responding to a question on debunking cyber-security myths, says "There are myths? ... There are a lot of bare thrust out there that people choose to ignore. Like the fact that while antivirus isn't perfect, it's still necessary. Like the fact that we've known how to build secure systems for 40+ years, but the economics and business motivations aren't there to do it."

To the same question, Steve Ragan, a journalist who covers national security and information security, responds that he "would like to see a few myths done away with. The first is that zero-day vulnerabilities [unanticipated software flaws] are the ultimate risk and should be one of the top focal points when developing a security program. That's just not true. In fact, most attacks will originate via phishing, exploiting weak and improper controls, or leveraging existing [old] vulnerabilities." This 417-page book is particularly helpful for those considering a career in the cyber-security field, whether as a startup or an entry-level employee. Tribe of Hackers is also a useful reference source for cyber-security practitioners throughout the world. For many readers, this book will likely confirm preconceptions they may have, while deepening their understanding of other facts and unpacking some myths from the cyber world.

Left:
Marcus J. Carey and Jennifer Jin