

Zero Trust in Healthcare Delivery Organizations (HDOs): Switch from Traditional Model to ZTA

Aaddya

School of Sciences, CHRIST (Deemed to be University), Ghaziabad, Uttar Pradesh, India

Dr. Shilpa Srivastava

School of Sciences, CHRIST (Deemed to be University), Ghaziabad, Uttar Pradesh, India

Dr. Madan Singh

School of Sciences, CHRIST (Deemed to be University), Ghaziabad, Uttar Pradesh, India

Abstract

In recent times, many healthcare centers faced consequences due to latest technologies, distant work setups, and the need for cybersecurity in healthcare. Older security measures used to work on specific perimeters does not protect sensitive healthcare information because attackers easily find vulnerabilities in healthcare data.

Due to these challenges, cyberattacks on healthcare has increased, with attacks such as ransomware, data stealing. And also, there are few government laws on how healthcare data should be protected. This made clear that traditional security methods where we “trust” insiders and protect system from outsiders are not reliable.

Because of these issues “Zero Trust Architecture” were introduced. These uses continuous verification in each step to protect patients’ data from cyberattacks, such as ransomware and data stealing. This approach of “Zero Trust & Continuous Verification” helped to create more secure system, which is used to protect the healthcare data.

Keywords

Zero-Trust, Cyberattacks, Healthcare, Data Stealing, Ransomware.