

## **Financial and Health Benefits of EHR Implementation**

Implementing EHRs has several financial and health benefits to healthcare organizations, providers, and patients. On the financial aspect, EHR systems can help to minimize operational costs by limiting paperwork, streamlining workflows, and enhancing the accuracy of billing. Keshta & Odeh (2021) note that healthcare providers who adopted EHRs in their facilities observed savings in charting expenses and transcription services. Moreover, EHRs optimize the management of the revenue cycle by reducing and improving reimbursement rates and claim denials.

Healthwise, EHRs have played a significant role in improving the coordination of care and patient outcomes. Since they enable real-time access to patient records, EHRs empower providers to make informed decisions, minimizing unnecessary duplicate testing and errors. In addition, EHRs support preventive care by offering reminders for vaccinations and screenings. Patients also benefit from the use of EHRs improving engagements through patient portals, which not only provide access to health records but also promote better communication between patients and patients (Murdoch, 2021).

### **Cost of Implementing and Managing EHRs**

The initial implementation of an EHR requires intensive capital, including the cost of acquiring the software, hardware upgrades, workflow redesign, and training. Keshta and Odeh (2021) estimate that for a small-to-medium-sized practice facility, the initial costs for implementing a EHR may range from \$33,000 to \$162,000. However, the price may reach millions of dollars for larger healthcare systems.

Additionally, the long-term management of EHRs may also incur costs that include IT support, subscription fees for cloud-based systems, system updates, and cybersecurity measures. Precisely, Kalinin (2024) suggests that healthcare organizations should expect to spend about 15-20% of the initial cost of EHR implementation on annual maintenance. For example, an EHR software that costs \$100,000 to initially implement, requires a budget of around \$15,000 to \$20,000 yearly for maintenance.

### **Current Security Concerns Surrounding HIT and EHRs**

Although EHRs have significant benefits, there are also security challenges that result from their use. For instance, healthcare organizations have faced constant cybersecurity threats such as data breaches, ransomware attacks, and phishing campaigns, jeopardizing patient privacy. According to Kalinin (2024), more than 50 million patient records were compromised in the United States alone in 2022 due to cyberattacks.

Internal threats have also made EHRs vulnerable through practices such as accidental disclosures and unauthorized access by employees. Therefore, ensuring the data is secure requires robust measures such as multi-factor authentication, encryption, and regular security audits. In addition, organizations must align their practices according to established protocols for disaster recovery and data backup to minimize the effect of potential breaches (Murdoch, 2021).

### **Federal Legislation and HIT: The HITECH Act**

The HITECH Act of 2009 was an important legislation to foster the adoption and meaningful use of HIT, such as EHRs. The Act resulted in the allocation of billions of dollars to empower healthcare providers to adopt certified EHR systems and achieve specific benchmarks in their use. Under HITECH, a significant requirement is adherence to

"Meaningful Use" criteria, which stresses enhancing safety, quality, and efficiency while minimizing health disparities. For instance, providers must show their ability to share patient records electronically, e-prescribe, and report quality metrics.

Moreover, HITECH strengthened HIPAA regulations through the introduction of the Breach Notification Rule, which makes it mandatory for healthcare organizations to notify affected individuals, that is, the Department of Health and Human Services (HHS), and, in some cases, the media in case there is a breach involving protected health information (PHI). Failing to comply with these requirements attracts huge fines, highlighting the significance of implementing robust EHR security (Mahajan et al.,2021).

APPLEWRITERS.COM

## References

- Kalinin, K. (2024, January 8). *EHR Implementation Cost Breakdown: Uncovering the Hidden Expenses*. Topflight. <https://topflightapps.com/ideas/cost-of-ehr-implementation/>
- Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177-183.
- Mahajan, S., Lu, Y., Spatz, E. S., Nasir, K., & Krumholz, H. M. (2021). Trends and predictors of use of digital health technology in the United States. *The American journal of medicine*, 134(1), 129-134.
- Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*, 22, 1-5.