HealthManagement
Promoting Management and Leadership

Navigating the Risks and Rewards of Remote Patient Monitoring

Remote patient monitoring (RPM) is revolutionising healthcare, allowing patients to receive care at home while providing healthcare providers with real-time data. This shift in healthcare delivery has seen increasing adoption among hospitals and health systems, driven by the potential for enhanced patient outcomes and reduced hospital readmissions. Efforts by the CPT Editorial Panel and the American Medical Association may soon expand reimbursable RPM services, further incentivising its use. However, the integration of RPM into healthcare also introduces significant risks, including data breaches, device malfunctions, missed readings, and critical financial losses. To successfully adopt RPM while mitigating these risks, healthcare providers must adopt comprehensive strategies.

Identifying Key Risks in Remote Patient Monitoring

According to Justin Kozak, life sciences lead at Founder Shield, three major risks are associated with the use of RPM technology: data security and privacy, the potential for misdiagnosis or missed events, and overreliance on technology.

Data Security and Privacy: RPM systems collect vast amounts of sensitive patient data, making them prime targets for cyberattacks. Ensuring robust data security is paramount, as breaches can erode trust and result in significant financial and reputational damage. Hospitals and health systems must invest in advanced security measures and adhere to cyber best practices to protect patient information.

Misdiagnosis or Missed Events: RPM can potentially lead to misdiagnoses or missed critical events due to reliance on algorithms and technical systems. The absence of a physical exam and potential technical glitches can result in inaccurate data interpretation. This can lead to delayed or inappropriate interventions, increasing healthcare costs and negatively impacting patient outcomes.

Overreliance on Technology: While RPM offers numerous benefits, overreliance can be detrimental. Healthcare providers may become too dependent on technology, neglecting the essential human element of care. Regular in-person assessments remain crucial to ensuring comprehensive and empathetic patient care. Overreliance also poses risks during technical outages or glitches, which can lead to severe consequences for patient safety and legal disputes for healthcare providers.

Mitigating Risks in Remote Patient Monitoring

To mitigate these risks, C-suite executives and technology teams must implement several key strategies:

- Invest in Robust Security Measures: Data security must be prioritised. This includes using state-of-the-art encryption, regularly updating software and firmware, and conducting frequent penetration tests. Additionally, training employees on data access and usage guidelines and partnering with secure, HIPAA-compliant technology vendors can significantly enhance data protection.
- Establish Clear Protocols for Data Interpretation: Developing stringent protocols for interpreting RPM data can help prevent misdiagnoses and missed events. Investing in high-quality RPM devices and platforms that prioritise accuracy and reliability is crucial. Regular in-person check-ups should complement RPM to ensure comprehensive patient assessment and care.
- Promote Responsible Use of RPM Technology: Ensuring that RPM is viewed as complementary to traditional care, not a replacement, is vital. Healthcare providers should maintain regular in-person interactions with patients to prevent overreliance on technology and to address any issues promptly. This balanced approach can enhance patient care while minimising risks.

Advice for Healthcare Leaders Considering RPM

For hospitals and health systems considering RPM, Kozak offers three key pieces of advice: start small and scale up, commit to education, and partner with experts.

- Start Small and Scale Up: Pilot RPM programmes with specific patient populations to refine protocols and test security measures. This phased approach allows for the identification and resolution of potential issues before full-scale implementation, building a strong foundation for broader adoption.
- Commit to Education: Continuous education on data and privacy regulations, as well as staying abreast of cyber trends, is crucial. Healthcare leaders should foster a culture of ongoing learning to ensure their teams are well-equipped to handle evolving challenges in RPM.
- Partner with Experts: Collaborating with digital specialists in cybersecurity, information technology, and other relevant fields can provide essential support and guidance. Building a strong network of experts can help healthcare providers navigate the complexities of RPM and enhance their overall risk management strategy.

While RPM presents significant opportunities for improving patient care, it also introduces new risks that must be carefully managed. By prioritising data security, establishing clear protocols, and fostering responsible use, healthcare providers can successfully integrate RPM into their care models, enhancing patient outcomes while minimising potential pitfalls.

Source: **Healthcare IT News**

Image Credit: **iStock**

Published on : Wed, 12 Jun 2024