Healthcare

ALERTBULLETIN®

A Risk Management Update | 2023 Issue 4

Remote Patient Monitoring: Five Basic Risk-reduction Strategies

Remote patient monitoring (RPM) refers to the use of wireless technologies to collect a wide range of health-related metrics – from blood pressure to sleep patterns to blood sugar levels – and to automatically transmit this information to providers. By amassing data on an ongoing, moment-by-moment basis, RPM may enhance many clinical tasks, including chronic disease management, post-hospitalization care and hospital-at-home (H@H) programs, whereby home-based patients are treated for acute conditions that traditionally required inpatient care.*

RPM tools – including both mobile medical devices (such as implantable cardiac monitors) and patient wearables (such as watches designed to track heart rate) – grew in popularity during the COVID-19 pandemic, due to overcrowding of hospitals and other healthcare settings, as well as the desire to reduce in-person visits. The upward trend in RPM utilization has continued, as the healthcare industry seeks to revitalize care processes in response to changing delivery models and reimbursement pressures. In fact, it is estimated that 70 million patients, or 26 percent of the U.S. population, will use RPM tools by 2025, more than double the 29 million users in 2020.

* In late 2022, H@H programs were first authorized by the federal government in an effort to maximize inpatient bed capacity of hospitals during the COVID-19 pandemic. The U.S. Department of Health and Human Services has since extended the period in which hospitals can apply for H@H program waivers to December 31, 2024.

Did someone forward this newsletter to you? If you would like to receive future issues of *AlertBulletin*® by email, please register for a complimentary subscription at go.cna.com/HCsubscribe.

Although many patients and providers have embraced the benefits of RPM devices, the technology also is replete with associated limitations and risks. (See "Remote Patient Monitoring: Pros and Cons" on page 2.) Furthermore, the regulatory framework, standards of care, and provider roles and responsibilities pertaining to RPM are still evolving, requiring providers and organizational leadership to remain abreast of changing state and federal laws, as well as professional guidelines.

To help healthcare organizations and providers protect themselves against RPM-related liabilities, ranging from faulty data to diagnostic errors to device misuse and malfunction, this edition of *AlertBulletin*® focuses on five risk control strategies:

1. **Select user-friendly devices** that have been tested for reliability, accuracy and safety.
2. **Educate providers and staff about properly using RPM tools** and interfacing with IT systems.
3. **Work with internet-savvy patients** who are willing and able to actively manage their health.
4. **Decide how RPM data will be managed and by whom,** as well as how devices and systems will be audited and assessed.
5. **Be aware of relevant privacy and confidentiality rules regarding RPM-generated data** and implement effective security measures.

1 Basic Device Considerations

There are two major categories of RPM tools: medical and consumer grade. Medical-grade devices – such as ventilators, apnea monitors, infusion pumps and blood glucose meters – are available solely by prescription. These tools undergo rigorous FDA design verification to ensure their clinical safety and effectiveness. *Consumer-grade devices* – including watches, earbuds, wrist and ankle bands, and other over-the-counter wearables designed to promote wellness – do not require FDA clearance. They are subject to a less vigorous pre-market review, which may consist simply of the manufacturer's assurance that the product performs as described. Hence, they tend to be more variable in terms of performance.

Laws and regulations are evolving with respect to whether a consumer-grade device that is recommended rather than prescribed – e.g., a wearable Fitbit worn by a patient diagnosed with atrial fibrillation – establishes a duty to monitor on the part of the physician. As a rule, consumer-grade wearables should be incorporated into a patient's plan of care following consideration of such questions as how often data will be reviewed and whether findings will be factored into the clinical decision-making process.

Remote Patient Monitoring: Pros and Cons

Pros:

- **RPM offers providers continuous access to vital signs,** enabling early detection of changes in condition.
- **Use of RPM tends to increase patient engagement** and facilitate a more collaborative approach to healthcare.
- **Automatic monitoring may help reduce costs** by decreasing the need for in-person patient encounters.
- **Enhanced tracking of health status can lead to fewer hospitalizations,** as well as overall better patient outcomes.

Cons:

- **RPM technology is not foolproof,** and misuse or overreliance may lead to diagnostic and treatment errors.
- **Compiling vast amounts of patient data may be counterproductive,** potentially overwhelming staff and providers.
- **Patients may resist and/or resent constant monitoring,** straining relationships with providers.
- **Users require access to a smartphone with broadband capabilities,** which may exclude some patients.
- **RPM data must be redirected to organizational IT platforms** and/or electronic patient record systems, presenting technical challenges.

2 Education and Training

Healthcare organizations that utilize RPM tools must create written parameters for their use and communicate these protocols to providers and staff. Orientation and educational sessions should focus on the following key areas, among others:

- **Scope of RPM services** and data monitoring responsibilities.
- **Informed consent process,** including the provider-patient discussion about RPM use and documentation requirements.
- **Verification of the device's basic functionality,** as well as the accuracy of transmitted data.
- **Data monitoring guidelines,** including frequency of data review, policies for notifying physicians/providers in emergency situations and documentation requirements.
- **Integration of data into IT platforms,** including the electronic healthcare record (EHR) system.
- **Patient communication** and follow-up.
- **Device malfunction response,** including reporting protocols.
- **Risks of overreliance on RPM findings** and artificial intelligence-generated outcomes.
- **Discontinuation of services,** including patient notification and documentation of reasons.
- **Confidentiality issues** and measures to safeguard data.

Ensure that all staff and providers involved in remote monitoring activities are conversant with the specific devices and their permitted uses, and that they have been trained in healthcare data privacy rules and related security training. Document proficiency testing in personnel files.

Both patients and staff require education on the scope of RPM services. In addition to providing hands-on training in the use and maintenance of the monitoring device, ensure that patients are informed about the following treatment-related matters, among others:

- **The specific data to be monitored,** transmitted and analyzed.
- **Timing and duration of RPM use,** e.g., between provider office visits, until hospital readmission for episodic conditions or on a lifelong basis for chronic care patients.
- **Frequency of data review** by providers or qualified staff members.
- **Proper response to device alerts,** as well as an explanation of what constitutes an emergency reading.

- **Available hours for provider consultation,** in the event of abnormal findings.
- **Emergency response measures,** if no staff member or provider is readily available to respond to abnormal readings (i.e., call 911 or seek treatment in an emergency care setting).
- **Device malfunction indicators,** as well as consequent reporting procedures.

Discussions on these subjects should be documented in the patient healthcare information record.

3 Patient Selection

Not every patient is a suitable candidate for remote monitoring. The selection process should include a range of criteria, both health-related and technical. RPM is most suitable for patients who are …

- **Undergoing medical care involving easily trackable metrics,** such as diabetes management; heart, lung or blood disorders; sleep problems; weight loss monitoring; fall mitigation; and medication-assisted therapies in substance abuse treatment programs.
- **Motivated to actively manage their health** and to collaborate closely with providers.
- **Capable of operating the device in a safe manner,** as well as checking and maintaining it.
- **Equipped with a smartphone** and have adequate access to the internet.

Patients who qualify for remote monitoring by a medical-grade device must give their consent before its use can be initiated. (See "Medical Grade Devices: Elements of Informed Consent," at right.)

4 Data Management

The effectiveness of remote monitoring depends, in large part, upon the ability of the device to interface with EHR systems and other clinical IT platforms. Ideally, data should stream directly into the EHR, enabling staff to track findings via a convenient dashboard format. By appointing a qualified healthcare professional to monitor and respond to incoming data, facilities and medical offices help to ensure prompt review and also diminish the risk of "alert fatigue" for providers subject to receiving multiple simultaneous high-priority messages.

In addition to integration with existing IT systems, sound data management requires close attention to workflow and quality control issues. The following questions are designed to help providers and organizations establish effective protocols for collecting and utilizing RPM-related data:

- **Who will manage the device** – the provider, healthcare organization or vendor?
- **Which member of the treatment team will review incoming data and device alerts,** when and how often?
- **Will third parties have access to the data,** and is protected health information secured against improper disclosure?
- **Is a schedule established** for monitoring patient data?
- **Are there sufficient staff to manage incoming data,** especially if a device is transmitting on a 24/7 basis?
- **Is there a formal alert policy** specifying when providers will be notified of abnormal readings?
- **Is there an audit mechanism** for reviewing clinical decisions supported by RPM data, in order to ensure the accuracy of data and the appropriateness of responses?
- **Does the audit process note whenever a provider overrides RPM findings** and/or software-driven diagnoses or treatment recommendations?

Medical Grade Devices: Elements of Informed Consent

Informed consent discussions involving FDA-approved RPM tools should include the following elements, among others:

- **Description of what the monitoring device does** and how it will support the treatment plan.
- **Benefits and risks of RPM,** as well as possible alternative therapies.
- **Use and maintenance guidelines** for the patient.
- **Frequency of data monitoring** and review of findings.
- **Alert response protocols** and management of emergency readings.
- **Device limitations,** in terms of both accuracy and reliability.
- **Technological concerns,** including connectivity issues and the possibility of device failure.
- **Data confidentiality risks** and privacy safeguards.
- **Discontinuation rights of patient and provider,** i.e., how and when either party may terminate the arrangement.

5 Privacy Protections

Remote monitoring tools have an inherent exposure to cyber liability. Device manufacturer safeguards provide some measure of security, but medical offices and other healthcare settings must implement their own strategies to protect patient privacy and limit potential exposure, as suggested below:

- **Adopt a comprehensive range of technical safeguards,** including password-protected access to software applications, end-to-end encrypted data transmission and data access restrictions.
- **Install antivirus software and firewalls** designed to detect and neutralize viruses and malware that may potentially compromise the confidentiality, integrity and availability of RPM data.
- **Comply with HIPAA privacy and security requirements,** as well as FDA guidance on medical device cybersecurity risks.
- **Include RPM activity in the organization's security management plan,** as well as the annual HIPAA security risk assessment.
- **Reference RPM-related data breach risks in the HIPAA Notice of Privacy Practices** presented to patients before every healthcare encounter.
- **Have legal counsel review business associate agreements with vendors** to ensure compliance with federal and state privacy and confidentiality requirements.

Remote patient monitoring technology is developing rapidly, while associated regulatory structures, standards of care, and organizational policies and procedures lag behind. The five strategies described in this publication can help providers, medical practices, allied healthcare facilities and hospitals evaluate their current RPM-related practices and ensure that these high-tech tools are being utilized in a safe, consistent and compliant manner.

Reducing the Risk of RPM Device Malfunction

- **Evaluate the safety, reliability and accuracy of mobile devices and wearables** before prescribing or recommending them to patients.
- **Remain up-to-date on manufacturer warnings,** as well as device safety records and approved uses.
- **Assess internet connections** prior to dispensing devices.
- **Check medical device websites frequently** and respond promptly to FDA alerts or device recalls.
- **Ensure that vendor contracts specify each party's responsibilities** in the event of device malfunction.

Quick Links

- Feske-Kirby K, et al. "Using Machine Learning to Improve Patient Safety in the Home or Remote Setting for Adults." Patient Safety Network, February 15, 2023.
- Hood, C. et al. "Remote Patient Monitoring." Patient Safety Network, March 15, 2023.
- Remote Patient Monitoring: Implementing RPM in Practices, issued by the Harris County Medical Society.
- *Remote Patient Monitoring Playbook*. American Medical Association, 2022.
- "Remote Patient Monitoring (RPM) Toolkit." The National Consortium of Telehealth Resource Centers, November 30, 2020.
- "Telehealth and Remote Patient Monitoring." A resource page from the Department of Health and Human Services, on Telehealth.HHS.gov.

For more information, please call us at 866-262-0540 or visit www.cna.com/healthcare.