Remote Patient Monitoring (RPM) – Security and Other Adoption Barriers

Source: Alisa L. Niksch, M.D., Brian S. Rothman, M.D., and Steven J. Davidson, M.D., M.B.A.

This brief examines the current obstacles within the healthcare environment and new challenges presented by the use of digital technologies for remote patient monitoring (RPM). The content is intended to provide a realistic perspective of the barriers that currently exist in order to help the reader not only avoid or overcome them before implementation, but ultimately realize the benefits that can come from RPM and digital health. The vast transformation potential for digital health technology to create a more patient-centric healthcare system, decrease costs, and improve outcomes has been outlined in a companion HIMSS document, “The Value of Remote Patient Monitoring (RPM): A Physicians’ Perspectives”.

Digital Remote Patient Monitoring Technologies Adoption Barriers

A myriad of factors within the current healthcare ecosystem obstruct RPM digital health solution adoption. These factors are interrelated but can be placed in distinct categories. An awareness of the interplay between clinical, economic (including reimbursement models) and social environments is crucial to effectively integrating RPM systems into routine patient care.

Scalable business model barriers: Evidence supporting a scalable business model for RPM tools is scant, presently. Industry startups rely upon provider focus shifting from fee-for-service to risk-based revenue sources. Enterprise and practitioner level providers are uncertain and anxious about deployment because of RPM’s overwhelming data stream volumes and the associated increase in liability. Alternatively, those who believe in this decade-old market are investing in their businesses’ technologies and marketing expecting robust future revenue growth. Medical centers and health systems are partnering with early stage digital health companies to perform monitoring platform pilot studies viewed as key for building future credibility in this market.

Demonstrating efficacy attracts investment dollars. One example is the partnership between AMC Health and Geisinger Health System, New York Health and Hospitals Systems, and Health Partners of Minnesota. AMC’s platform of telehealth services, health monitoring and coaching, and data analytics, has been implemented with great success. Other companies, including MC10 and Zephyr™ Technologies, have partnered with Pharma Company UCB and University of Arizona Medical Centers, respectively, to develop new use case scenarios and conduct validation studies. [Please note that inclusion or exclusion of any vendor products within this or any HIMSS document does not imply any level of endorsement. These references are merely used for demonstrative purposes.]

Patient adoption barriers: Consumers appear to be keenly interested in the wearable sensor market, but have not yet committed in a significant way to take advantage of these products. Cost factors - A Pricewaterhouse Coopers Health Research Institute report from 2014 revealed that only 21% of survey respondents owned a wearable, and only 10% used one daily. Further, 38% would spend up to $100 for a wearable device, and most (68%) were willing to use a wearable if their employer or
insurance company provided it in exchange for premium discounts.

**Demographic and infrastructure challenges:** Installing this technology into consumers’ homes that may not have a wireless network or smartphone would likely be a futile exercise. Further, Wi-Fi and cellular signals can be unreliable and patients and their caregivers are ill equipped to troubleshoot to regain connectivity. Implementing RPM technologies including wireless scales and blood pressure cuffs have been accomplished at Ochsner Health System in New Orleans. However, the support necessary to achieve this result in the elderly population studied is not clear from the published abstract. Finally, many RPM technologies do not employ assistive technologies for those with hearing, vision, or motor impairments.

**Physician adoption present barriers:** Numerous physician workflow factors are obstacles to RPM technology adoption. Any of the following might impact adoption and one highlighted for planning purposes:

- **Lack of clinical validation** — The reliability of data collected through devices that may not be FDA approved and the implicit demand for parsing “too much data” are common physician concerns. Further, many clinical studies lack the power to prove clinical efficacy and most lack the power to prove cost savings. Effective patient generated health data consumption will require a means for providers to screen, select and verify RPM data in the EHR so that practitioners commit meaningful data. This will enable them to be better partners to their patients rather than feeling overwhelmed.

- **New technologies** — The Intimidation factor — EHRs already exhaust physicians with depersonalization and increased documentation burdens. Physicians may unjustly assume that digital RPM platforms will result in similar headaches. These assumptions make clinician collaboration difficult and complicate technology development and validation to prepare platforms for commercialization.

- **Data Overload Risk** — Unfiltered patient data may increase patient risk because physicians may be required to locate actionable data (signal) within an overwhelming amount of artifact (noise) including false positive alerts. In addition, inadequate or absent integration of data analytics and intelligent notification protocols into RPM platforms can undermine a wireless medical device or app’s effectiveness by increasing physician workload, inefficiency, and risk. Unfiltered patient data increases risk to physicians who are tasked with finding actionable data within a stream of useless or faulty information.

- **Lack of interoperability with EHR platforms** — The term “information islands” has been used to describe subsets of patient data isolated from the bulk of patient historical data. The lack of interoperability between devices and systems creates transient data sets, secondary in value.

- **Institutional barriers:** Poor integration into complex workflows — Enterprise RPM adoption is slow because of the overwhelming burden of other IT initiatives (Meaningful Use, ICD -10, etc.) and uncertain ROI. Intelligent data filtering is necessary, so applying the “quantified self” concept to present unlimited physiologic data back to providers is incompatible with large health systems’ workflows. Data analytics providing risk assessments, condition identification, and intervention recommendations are lacking, owing to both a paucity of integrated platforms and algorithmic regulatory requirements when treatment modifications are recommended. Validation and verification of patient provided data is another system challenge, as verification of patient identity is crucial in ensuring both accuracy and security.

- **System deployment issues:** Delivering, installing, validating, and training are challenges that require on-site effort. Most institutions that implement digital health and RPM systems rely heavily on in-house IT specialists. The speed and extent to which on-site support may be mobilized varies
widely. External support and additional software integration services are uniformly costly and present a wide range of technical challenges.

**Patient and physician technical education and training:** While subsets of the patient adoption / physician adoption issues addressed above, institutions, ACOs, and hospital systems will ultimately grapple with some proportion of this responsibility. Training patients and their caregivers to use devices and backend software requires support “at the elbow” for all users with a duration of support dependent upon user capabilities.

**Resistance to research investment:** Academic institutions are the most favorable environments to introduce innovations in medical technology due to their research culture and interest in advancement. However, digital health technologies are not typical areas for clinical investigation. Financial barriers to funding research in this sector, which often involve young companies, abound and require substantial creativity from physician champions of these technologies.

**Legal and regulatory issues:** RPM technology innovation is developing more quickly than policy and legal responses, creating uncertainty for the market, practitioners and patients alike.

**FDA Oversight** – The FDA has established regulatory processes for digital health platforms that either directly controls wireless medical devices for RPM, or store and forward data from these devices. There is also regulatory enforcement of mobile apps that provide patient-specific diagnoses. These regulated functions are essential in the functionality of a monitoring platform to support clinician decision making processes. Insufficient funding, evidence, or time, emerging digital health companies can sink under the weight of these regulatory processes.

**Security breaches and liability** – Sharing of clinical information between health care providers and patients through digital media offers benefits to both doctors and patients, including improved coordination and efficiency in service delivery, reductions in medical errors and misdiagnoses, and convenience. However, this step forward poses unavoidable risks, particularly because different modes of digital communication are variably secured. In addition, mobile devices storing clinical information are portable and can be easily lost or stolen. Enthusiasm for these digital health tools exists in tension with privacy concerns, as data collected, stored and analyzed to the patient’s benefit may fall into others’ hands regardless of security efforts. A patient’s protected health information (PHI) on a mobile device or accessible through the device can also lead to security breaches of other patient private information, including financial and other personal records. The HIPAA Final Rule effective as of March 2013 places the burden of securing protected health information (PHI) squarely on physicians and healthcare organizations. Most importantly, loss of patient control over confidential and sensitive health information threatens the confidential communication between doctors and patients that has been a bedrock principle of modern medicine. Confidentiality ensures that patients seek out care, and that they are open and honest with their providers. Ultimately impacting all stakeholders in the healthcare ecosystem, patients who fear a loss of control over their private medical information may lose faith in their doctor, their hospital—and in the health care system itself.

Privacy and security in digital information collection, storage and utilization for patient benefit is dependent upon both technologies and behaviors. Patients and caregivers should be educated as to what data are collected through these platforms, to what purpose, how these data will be used and what other users and entities will have legitimate access to these data. A diabetes monitoring platform, for instance, may share clinical data with the physician, diabetes nurse educator, nutritionist, and general health coach, with options to share information with a family caregiver. Guides summarizing this information and sources for obtaining additional information should be available to the patient and patient’s caregivers. Optimally, technology recommended for RPM by clinicians should contain patient controlled privacy settings to determine who has access to data.

**Security solution pitfalls and mitigating risk** – Passwords and firewalls are simple IT solutions
that provides marginal PHI protection at best. When these fail, data encryption has been more widely implemented to mitigate risk of security breaches. Data encryption at rest is a basic expectation if data storage falls outside a healthcare organization’s oversight—whether through public, contracted cloud services or through a vendor’s privately owned storage resource. Database layer data encryption may be appropriate if there is a risk that physical hardware may be stolen or if the hardware is in a hardened data center. However, use of database layer encryption may not appreciably mitigate disclosure risks\textsuperscript{4}. If implemented, the technology of such encryption should assure that encryption keys are kept separate from the data, and should be based on an overall risk assessment, just as with encryption during transmission.

Confidentiality, as used in the privacy rule of HIPAA, pertains mostly to the means of communicating private health information between patient and provider. However, advocacy groups and organizations which speak on behalf of patients such as the NY-ACLU\textsuperscript{1} and PatientPrivacyRights\textsuperscript{2} include in their discussions of confidentiality the practice of restricting data access. That is, limiting access to the fewest number of data elements by the fewest authorized users for only authorized purposes. While current regulations don’t require this level of granularity in data control, both competitive advantage and perhaps regulatory pressure may drive future RPM development to deliver this type of control over patient data.

**Reimbursement issues**: The absence of reimbursement structures creates obstacles across the entire healthcare ecosystem. Non-reimbursable RPM technologies face funding challenges from reluctant investors. Patients resist paying for these products and services, physicians hesitate prescribing them, and institutions find it difficult to endorse them. While some interventions are reimbursable as “Chronic Care Management” (CPT 99490), widespread physician adoption may depend upon risk based compensation. At the enterprise provider level, RPM deployment is spotty and only used when other offsetting economic losses make it worthwhile (e.g., avoiding patient readmissions) until risk based compensation makes further inroads\textsuperscript{7}. Despite recent modifications, economic incentives in the U.S. healthcare system are not yet aligned with widespread use of remote patient monitoring. Fee-for-service models continue to disproportionally reward inpatient care and recurrent outpatient, in-person encounters.

**Conclusions**

The barriers to adopting digital health solutions for remote patient monitoring are daunting, and overcoming them will require tireless physician leadership. If physicians do not play a key role in the healthcare ecosystem surrounding emerging healthcare technology, the tools are unlikely to develop into viable, effective, commercial products. Clinical trials, championing innovation within health systems and institutions, and providing clinical context to digital platform developers of remote patient monitoring systems are just a few of the potential contributions physicians can make. Physician partnership and collaboration to develop RPM technologies is absolutely necessary to improve workflow, efficiency, and most importantly, effect a beneficial change in patient outcomes.
References:


5. U.S. Department of Health and Human Services: Health Information Privacy.


http://www.hhs.gov/news/pr