AMIA

INFORMATICS PROFESSIONALS. LEADING THE WAY.

December 21, 2018

Ms. Andrea Arbelaez
National Cybersecurity Center of Excellence
National Institute of Standards and Technology

Submitted electronically: hit_nccoe@nist.gov

Re: Securing Telehealth Remote Patient Monitoring Ecosystem

Ms. Arbelaez:

The American Medical Informatics Association (AMIA) writes to express our support for the National Cybersecurity Center of Excellence project, "Securing Telehealth Remote Patient Monitoring Ecosystems," and the development of a reference architecture that will address the security and privacy risks for healthcare delivery organizations leveraging remote patient monitoring (RPM).

AMIA foresees a future of care delivery and disease management that will rely heavily on RPM. A confluence of shifting and/or diminished reimbursement, aging and chronically ill population growth, and continued depopulation of rural areas will usher increased demand for remote sensing devices and systems. Securing these systems and ensuring trust in the data generated by these systems is an utmost priority, and is at the heart of consumers' ability to obtain care and manage their health.

During our 2017 Policy Invitational we focused on identifying the characteristics of a person-centered – rather than an institution-centered – informatics infrastructure.[1] Attendees identified a problem statement entitled, "Data Sources Across Home & Community," which stated: Data sources for care, research, wellness, and community will continue to proliferate. There is a lack of coordinated capacity for data collection (from all types of sources) across home and community.

To address this problem, attendees recommend that "A public-private collaborative should develop an infrastructure and governance framework that (1) recognizes the diverse and proliferating data from home to community sources and that (2) provides mechanisms for data source identification, registration, and production of relevant metadata for the appropriate re-use of such data."[2]

We view this work as aligned with these recommendations and would like to offer AMIA member expertise as a resource. Numerous members are working to deploy RPM on behalf of their health system and many others are working on projects with companies who develop RPM solutions. Below, we offer a sampling of feedback, generated by AMIA members with such expertise.

[1] https://www.amia.org/sites/default/files/API-2017-White-Paper-Redefining-our-Picture-of-Health.pdf
[2] Ibid.

First, we premise the following by articulating our view of security as ensuring data is seen only by those who are authorized to see such data and that those data have not been corrupted in any way.

Second, we strongly urge this work to utilize the commodity mobile infrastructure already in place, rather than some health specific standard to be economically viable. The ultimate spread, scale, and usage of these RPM tools will likely depend more on the commercial marketplace than the short- and long-term plans of healthcare institutions. Further, patients/consumers will use the tools that they are familiar and fits best into their individual "workflows." Securing the existing mobile infrastructure where individuals perform most of their day-to-day living will improve the likelihood that healthcare specific tasks will succeed.

Third, we note that Singapore has published a standard / technical report on RPM,[3] which may help inform this work, and we note that both HL7 and IHE are working to develop standards for RPM that leverage FHIR.[4,5]

Lastly, an RPM infrastructure that provides data provenance will be important to enable clinicians and health systems to trust the data is accurate and unchanged from its origin.

In addition, we offer the following recommendations and observations:

- There needs to be a way to vet the RPM companies for security vulnerabilities - if this is beyond the scope of the proposal, then the proposal should at least define the framework to be used for the vetting (what should reviewers evaluate?)
- Data should be stored and transmitted encrypted
- If possible, the data packet structure should be standardized to enable determining whether a data packet has been altered; this is less important for "number of steps," but this becomes important when data like glucose level are transmitted; if a modification can be performed without being detected as a change, clinical action taken could be harmful and if that was the intention of the cybercriminal, patients could be harmed or killed; we know many instances where action has been taken based on a computer reading because computer readings are inherently trusted
- Data packets should include time of measurement and use UTC so each geography can adjust accordingly; it should be clear when a measurement was taken
- Standard unit definitions should be used for reporting and included with each datum; 2.3 is not sufficient even if the device only measures one thing, the data packet should say something like 2.3 meters per second

[3] https://www.singaporestandardseshop.sg/product/product.aspx?id=92a55ad9-d422-4352-b375-e44ae5e615cf
[4] https://healthcaresecprivacy.blogspot.com/2018/04/ihe-on-fhir-tutorial.html
[5] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=33

- Data units should have standard descriptions so there is no confusion as to whether "meters per second" is the same as "mps"
- Both companies and each individual monitor need a standardized unique identifier that follows a defined pattern (e.g. 4 bytes for companies and 8 bytes for devices); all transmitted data should include both (company & device) identifiers to enable easier long term clinical data management and after-market reporting

AMIA supports the NIST process and encourages a focus on data security and integrity that provides data provenance and supports consistent semantic meaning of the data across RPM manufacturers. Should you have any questions or require additional information, please contact AMIA Vice President for Public Policy Jeffery Smith at jsmith@amia.org or (301) 657-1291 ext. 113. We, again, thank NIST for the opportunity to comment and look forward to continued dialogue.

Sincerely,

Douglas B. Fridsma, MD, PhD, FACP, FACMI
President and CEO
AMIA