Recent advancements in sensor technology have paved the way to increase the effectiveness of body area networks (BANs) at building and updating comprehensive medical records of their users. Unsurprisingly, the wealth of information that can be obtained by performing analytics on these records are highly valuable. For instance, the city of New York was able to stymie the spread of tuberculosis by pinpointing the areas of the city with higher rates of infection and optimizing their resource distribution accordingly [1]. Though the importance of health analytics can not be understated, there are several concerns researchers must address before users are willing share their data, chief among which include privacy.

Even assuming the safe transmission of medical records, which include private information such as sexual orientation and body weight, via encrypted channels, researchers must first decrypt them before processing. At this stage, individual records are susceptible to snooping by not only the research team and staff, but also by the curious servers on which they are stored.

Similarly, loss of ownership, characterized by the inability of users to dictate the use of their data, is also a major concern. Understandably, users often assume that their records will be used by researchers only within the scope of their study, but doing so is often fallacious.

Finally, while the burden of participation is not an issue that directly affects the well-being of users, it negatively impacts participation rates, and remains a valid concern. Current solutions such as secure multi-party computation (SMPC) are cumbersome for users, requiring, for example, multiple rounds of communication or consistent internet connection for the duration of the study.

To overcome these issues, we propose using multi-input functional encryption (MIFE) [2]. As a variant of functional encryption, MIFE enables researchers to compute functions over a set of medical records without needing to decrypt them, assuming they have the correct function key. Furthermore, our solution allows users to verify, through inspections of the function keys granted, that researchers only use their records within the scope of their stated study. By using MIFE, therefore, researchers can take full advantage of the capabilities of BANs without jeopardizing the privacy of their users.

References
