Experimental Procedure Change Summary:

MIT Medical is currently undertaking a human participant experiment to conduct community testing within the MIT residential system to monitor and help mitigate spread of SARS-CoV-2. Related to this effort, the purpose of this amendment is to expand upon the MIT residential community testing COUHES protocol in order to incorporate privacy-preserving digital contact tracing in the MIT residential system via an MIT-affiliated contact tracing phone app.

Reason for Changes:

While manual contact tracing has been shown to be effective in mitigating the spread of viral infections, it requires significant human resources that do not scale well (e.g., large call centers) and relies on a diagnosed patient's memory. As recent discoveries about SARS-CoV-2 indicate that the time from infection to onset of symptoms can sometimes exceed 10 days (during which time the person is already contagious), patients can have difficulty remembering when and where they went and with whom they might have come in contact with. Consequently, we would like to incorporate digital contact tracing to address these drawbacks and mitigate the spread of SARS-CoV-2 within the MIT community.

Detailed Experimental Procedure Changes:

In order to augment manual contact tracing within the MIT residential system with digital contact tracing, we intend to integrate with an MIT-affiliated contact tracing phone app. We intend to develop the capability to enable contact tracing in indoor environments and then deploy the app within the MIT residential system. We specifically aim to monitor usage of highly utilized resources and facilities in the dorms, including: hall common bathrooms, common kitchens, the front desk, and laundry areas. This new effort will involve developing the hardware and software necessary to identify when residents are present in these locations and integration with the phone app. The hardware will be composed of "beacons" that utilize wireless communication (Bluetooth and/or WiFi) with the users' mobile devices to detect when that user is present. In addition to tracking when people use shared facilities through the stationary beacons, the app will also contain person-to-person contact tracking by phone-to-phone communication. Namely, the app will have the participants' phones emit anonymous identifier "chirps" via Bluetooth and also keep track of "chirps" emitted by everyone else's phones and received by a user. Each participant's device will then store all identifiers that represent the devices of the individuals the participant came near.

After the development phase, we will solicit voluntary participation from MIT residence hall members by asking them to download the app on their mobile devices (see the "Recruitment of Subjects" section for solicitation details). We will also ask each participant to provide the MAC address of their mobile device, which will be stored in an encrypted database on an MIT server. Once the app is downloaded and enabled, it will collect three pieces of information about the user's device: the make, the model, and the operating system version. This information will be added to the encrypted database. Time-stamped information about the participants' location within the common dorm areas as well as selected data from the participant's phone's sensors will then be collected and either stored on the user's phone or anonymized (i.e., having all direct personal identifiers removed) and stored on an encrypted database on an MIT server. The phone sensor data can include (based on the participant's particular phone model): accelerometer, gyroscope, magnetometer, proximity sensor, ambient light sensor, and barometer readings. These additional sensor readings will be used to help calibrate the contact tracing algorithms used in the app. The user's phone will also store the identifier "chirps" that it hears from other participant's phones. If the participant receives a positive diagnosis, they can voluntarily share this information and share their anonymized data with an MIT server if it has not been sent. This anonymized data will then be broadcast to other app users.

For each user, the location history of the infected person will be checked against the user's own location history. Furthermore, all of the identifiers emitted as "chirps" by the infected person will be compared to the list of identifier "chirps" encountered by the participant. If it is found that the user crossed paths with the infected person, the user will be notified only that they crossed paths with an infected person and within what distance and period of time this occurred (and will not be shown the location history of the infected person), and to seek medical advice from their healthcare provider. The distance and time thresholds that qualify a person as "crossing paths" with another person will be based on the most up-to-date data about transmissivity of SARS-CoV-2 (e.g., how long the virus can survive on surfaces after an infected person leaves).

The participants will also be asked to provide voluntary calibration data. This will involve participant-beacon and participant-participant calibration. For the participant-beacon calibration, the app will detect when a person is near a beacon (e.g., the person went to a shared kitchen) and occasionally ask the user to voluntarily perform a calibration step via an app notification. Namely, the user will be asked to go to the app, scan an RFID tag in the room (which will be clearly marked in each location with a beacon), and follow in-app, on-screen instructions. These might involve moving the phone in a specified way (e.g., in a circle), covering the front of the screen to block the ambient light sensor or trigger the proximity sensor, or another similar, simple task meant to help calibrate the aforementioned phone sensors. Each calibration is expected to take no longer than 2 minutes.

For the participant-participant calibration, participants will be asked if they currently live in a shared space (i.e., if they share an apartment or suite with other people). If so, the participants will be asked to voluntarily provide calibrations by following on-screen instructions in the app with their housemates. These instructions will ask pairs of participants to stand at specified distances from each other (e.g., 5ft, 8ft, 12ft) within their apartments and then pressing a button in the app to confirm when they are ready to record each distance. Each calibration is expected to take no longer than 2 minutes.

Finally, the participants will also be asked some questions via the app aimed at validating the digital contact tracing capabilities. Namely, when the user is near a beacon, they might receive a notification from the app asking them to voluntarily disclose how many other people are in the common area with them or if they are currently in a specific common area or not.

In addition to providing this enhanced contact tracing in support of mitigating the spread of SARS-CoV-2 within the MIT community, we also aim to leverage the resulting data to assess the effectiveness of the digital contact tracing system's "early warning" capability. This will be done by asking users to voluntarily disclose if they have received a warning from the app and if they also received a warning from a manual contact tracing effort and then comparing the time difference between the two warnings.

Finally, the wireless beacons will also collect time-stamped MAC addresses of all devices that come in their range. The MAC addresses are unique identifiers of the devices but do not directly identify the individual owners of these devices, and are continuously broadcast by devices such as phones during their normal operation. These data will then be encrypted and sent to an MIT server. The server will then check if the MAC address belongs to a participant who gave consent, and if so, it will store the timestamp and beacon ID in an encrypted database. These time-stamped MAC addresses will be used for verifying that the system is functioning correctly once deployed (e.g., to ensure that each beacon is "seeing" devices periodically) and for further potential analysis of virus transmission. This further analysis can be used as an additional source of risk assessment in order to provide a warning to the app users about their potential exposure to the virus.

Summary of New Benefits Based on Protocol Changes:

Immediate Benefits:

1. Digital contact tracing has the potential to improve the effectiveness of SARS-CoV-2 contact tracing within the MIT residential system, helping in the efforts to mitigate the spread of the virus within the MIT community.

2. Coupling digital contact tracing with broader medical testing under the original protocol will help assess the benefits and "early warning" capabilities of the digital contact tracing app. As the app is intended to be used outside of the MIT community in the future as well, this information will be critical in understanding how the app can be deployed outside of MIT to help mitigate the worldwide SARS-CoV-2 crisis.

Potential Benefits:

1. Understanding spread of the virus at a more granular level.

2. Experiment outcomes may provide helpful insights as to how MIT can possibly return to normal operations in the fall.

New Risks to Participants and Planned Mitigation Strategies:

1. Risk of disclosure of participants' private location history:

> Each user's location history will remain either stored locally on their phone or securely transmitted to an MIT server where it will be anonymized and encrypted. The private key used for decrypting this database will be stored on a different physical computer. For data stored on the user's phone, to further protect the user's location data, it will be stored in a secure storage location that is only accessible to the app. Therefore for an attacker to gain access to the user's location data, they would need to gain access to the MIT server to download the database and gain access to another MIT computer to get the private key used for decrypting the data. The only time the user's data moves from outside of their phone or outside of an MIT server is if they test positive and they provide consent that their location data be used to notify users with whom they crossed paths while potentially contagious.
>
> The collected time-stamped MAC addresses will also be protected. Namely, the data will be securely sent to an MIT server, where the sent MAC address will be checked against an anonymized list of MAC addresses of all participants. If the MAC address matches one from the list, the timestamp, beacon ID, and MAC address will be added to an encrypted database. The private key used for decrypting this database will be stored on a different physical computer. The list linking participants to their MAC addresses will also be encrypted and stored on a different physical computer. In summary, for someone to access the time stamped MAC address and the identify of who it belongs to, an attacker would need to gain access to the MIT server to download the database, gain access to a separate MIT machine to get the encrypted list of participants, and gain access to the private keys necessary to decrypt both files.
>
> To avoid personally identifying participants through the voluntary person-to-person calibration, only participants in residences with multiple shared apartments/suites will be asked for this data.

2. Risk of disclosure of participants' positive diagnosis:

Individuals who test positive need to opt-in to share their location data with other app users (and therefore self-identify as infected). Before the infected person's location data is checked against other users' location history, it will be anonymized and redacted. The shared list of identifier "chirps" of the infected person will be a list of anonymous identifiers that others cannot link to the individual. In order to minimize the risk of inadvertently identifying the infected person to the other users despite removing identifying information, their location history will not be shown to the other users; the only information they receive is if they crossed paths with an infected person, and within what distance threshold and time threshold this crossing occurred.