CONCORD®

VirAlert Enterprise

Enables real-time monitoring and analysis of COVID-19 infections in enterprise settings.

Given the global crisis induced by COVID-19, many employers are considering the eventual next step of reintroducing the workforce – whenever that day may arrive. As mandated lockdowns are eventually lifted, companies need a scalable method to monitor and analyze the health of their employees to prevent the spread of infection.

The VirAlert application suite is a multi-site scalable solution that emphasizes personal data protection while tackling exposure tracking, contacts tracing, and quarantine management.

FEATURE 1
REMOTE HEALTH MONITORING

Individual health monitoring becomes infinitely more challenging in large companies. Using VirAlert, employees are sent a daily reminder to answer a short health-based questionnaire. Likewise, the app offers a friendly chat bot interface to assist with self-diagnosis of symptoms and filter out non-risk conditions – this provides peace of mind for employees and helps lower the need for physical visits to overcrowded hospitals.

FEATURE 2
POTENTIAL CONTACT & DANGER ZONE ALERTS

Employees who have been in contact with someone with a confirmed infection need to be alerted immediately to avoid compromising anyone else in the workforce. By gathering anonymous data on the proximity of Bluetooth devices and correlating anonymous IDs with device owners, individuals can receive real-time alerts to avoid approaching areas and device owners with a confirmed case during the incubation period.

From there, the company can recommend individuals who were potentially in a danger zone self-quarantine for a set incubation period. Likewise, companies can manage quarantines using location and proximity-based technology, as an optional feature.

FEATURE 3
PERSONAL DATA PROTECTION

Most importantly, VirAlert believes in the importance of protecting personal data. All information is gathered anonymously and stored encrypted in a corporate data center that cannot be accessed by IT personnel. All stored data has a 21-day lifespan.

Only Bluetooth device addresses (BD_ADDR), information freely available to other devices anyway, is stored in the data center. The Bluetooth device address is only distributed to other devices in the event of a confirmed case or a contacted individual.