SMARTCONE
LEADING THE EDGE

Safe Entry with SYMP2PASS – Data Collection & Privacy Policy

Data Collection

Listed below is a general overview of the types of data collected from various SmartCone devices and the SYMP2PASS Pre-Screening Web Application:

1. Safe Entry with SYMP2PASS (Kiosk & Pre-Screening Web Application)
    a. Symptom Disclosure
        i. Symptoms of Infectious Disease (cough, fever, fatigue, headache, nausea, etc.)
        ii. Pre-existing Conditions (chronic cough, scent allergy)
        iii. Risk factors Associated with COVID-19 (exposure to a positive case, travel out of country)
    b. Video Intelligence
        i. Video with Artificial Intelligence data overlay (count, location of objects/people in the image, temperature measurement)
    c. Presence of Cough
        i. Voice Recording with cough detection
    d. Sense of Smell
        i. Ability to detect smell emitted
    e. Non-Personal Identification
        i. Synchronization of RFID tag in bracelet or key fob to pre-screening test results

2. SmartTorch
    a. Telemetry:
        i. GPS coordinates of people
    b. RFID Reader
        i. Non-specific identification through synchronization of screening results with RFID Key Fob or Bracelet

Sensors

Thermal Cameras:

- Thermal Bullet Camera paired with Blackbody
- Thermal Kiosk mounted camera

Cough Detection:

- Audio Recordings to detect cough

Sense of Smell Detection:

- ScentsiBLE Cards – QR code printed on peel or scratch and smell cards
- ScentsiBLE Sprayer – Scent emitted at Safe Entry with SYMP2PASS kiosks

Generated Data

- SmartCone offers all generated data to partners of the pilot program.
- No personally identifiable data is collected including name, gender, date of birth or address.
- It collects data from Video cameras, Microphones, RFID readers, and personal devices through the SYMP2PASS Web Application and Kiosks in standard format. This can be shared with customer as a recorded copy (optional feature).
- The SYMP2PASS Web Application requests location of the user at the city level to provide a map of public COVID-19 testing locations within the city for users flagged as being at risk.
- All thermal camera footage is stored on the local device. Sensitive data such as images of people being counted or screenings are only present on the sensor and discarded after analysis. Only the actual temperature reading and location data is stored with RFID tag information as anonymous data, and transmitted to the database.
- It also collects live telemetry data and shares it with the customer (optional feature) in real time. Information can be shared upon request.
- Operations team collects operational data with trouble tickets, issues found and metrics. This can be shared with pilot program partners as a recorded copy to generate final reports.

Cybersecurity

- System security is controlled by using least privilege accounts for operation and physical or application-based controls to limit access to software that can control the SmartCone.
- SmartCone follows the NIST (National Institute of Standards and Technology) Cybersecurity Framework of Identify, Protect, Detect, Respond, Recover.
- Security artifacts include system logs, admin use logs.
- *Aside from internal testing and verification, they have had penetration tests performed on the SmartCone systems to ensure security.
- Communication from the SmartCone to the cloud is done using TLS (transport layer security) transmission with independent certificates for each site to a secure endpoint.
- All access to data is through username/password and keys for API (Application Programming Interface) access over TLS secure communications.
- All software updates are testing in a development environment where SmartCone evaluates all changes made and ensure testing is done that follows all security guidelines.
- SmartCone uses individual partner cloud storage for each Safe Entry with SYMP2PASS deployment (ie. All data from the Durham Region Pilot will be stored separately from other customer data).

Personal Information

- SmartCone follows the official guidelines from GDPR (General Data Protection Regulation) which cover strict data privacy rules. They collect data related to the vehicle through sensors, and also collects camera data but store it for no more duration than permitted per the GDPR policy. SmartCone is willing to work with the project requirements in regard to guidelines established by FIPPA (Freedom of Information and Protection of Privacy Act) if required.
- SmartCone does not store or collect information directly related to the identity of any individual. All screening data is related to a QR code and RFID tag.
- Any Personal Information relating to the RFID tag is stored in encrypted storage with only SmartCone access. This data is then removed after a period of time unless it is required for analysis or evaluation of an incident.
- If screening results are needed to assess blocked entry into a building site, the site supervisor will have access to "pass/fail" information for each test and will not have access to audio recordings, specific screening and pre-existing condition question answers, or temperature reading values.
- Personal information is not stored in a method easily converted. Should the data need to be shared with 3rd parties, SmartCone would scrub the data of any personal information before providing.
- The SYMP2PASS data has been fully encrypted. Any breach of personal information data stored in the SmartCone would require decryption methods to get to the data for processing. Should a breach occur, SmartCone would notify the partners, specifying what data types were accessed.
- Data is securely transferred to the cloud for the purpose of auditing and improving the SmartCone system and software, and ensuring accurate results.