How Safe & Secure is My Child's Data?

Data & Personal Health Information (PHI) is very important to everyone at Imhealthytoday. We understand that a new program like this can raise several questions about the safety and security of your child's health and personal data. Rest assured that the professionals at Imhealthytoday are working hand-in-hand with your school to provide the maximum level of security for your child.

- The reality is the data collected to help protect the school community during the COVID-19 crisis is minimal & designed to capture only what is necessary for the overall protection of all children, teachers and staff.
- Most parents provide significantly more information with their children's physicals each year for sports participation than what is necessary to properly operate this program.
- The majority of data relates to current COVID-19 related symptoms (fever, cough, etc..) and has very low safety risks associated with the data.

Let's take a look at some common questions:

What is collected?

Daily Health Checker - Data collected and associated with the health checker falls into two low-risk categories:

(1) Census related such as: Name, address, parent's phone number & email address
(2) Current health symptoms status such as: dizziness, loss of smell or taste, headache, fatigue, sore throat, nausea, temperature

Medical Provider Telehealth Phone Calls - During a telehealth visit the medical provider may inquire as to the health history of the child. However, the majority of the discussion relates to the current health symptoms of the child or staff member so that the medical provider can help determine if COVID-19 testing is necessary and to be able to provide recommendations to the patient.

NO HEALTH DATA is shared with the school beyond the necessary results of COVID-19 testing. During health pandemics the importance of testing result knowledge at the employer or school level is greater than the privacy right of individuals to help protect the community as a whole.

What is not collected?

It is important to understand that "sensitive health information" is not collected or stored on the Imhealthytoday platform or in any way that is accessible to school officials.

- Items such as: social security numbers, physical health data related to diagnosed conditions, height, weight, blood type or other meta-data IS NOT COLLECTED OR STORED by IHT.

- Another positive aspect of the school's decision to engage doctors to help with its COVID-19 safety efforts is that all DOCTOR communications are regulated by the state and each Doctor's license. Schools are not put in the position of having to collect test results that could inadvertently become part of a student's permanent record.

Sharing of Data

Imhealthytoday is a joint venture between two doctor groups: *1.800MD* (a leading telemedicine doctors group based out of Charlotte, North Carolina) & *Elite Health* (a leading Concierge Medical Practice based out of Miami, Florida).

Educator-Resources, who is also working in partnership with ImHealthyToday, is a national brokerage consultant operating in all 50 US states to educate schools about special risk areas unique to schools and how to mitigate them. Educator-Resources is based out of Atlanta, Georgia.

Data Protection

- Only the census file (initial setup: ie: name, address, parent cell, parent email) is accessed by both Educator-Resources & Imhealthytoday.
- The COVID-19 immediate data (ie: initial and daily reporting or current health status) is only accessible by Imhealthytoday (not shared and not accessible by anyone else).
- When a medical professional is called in for a consultation with a member, the data is only accessible by the medical professional and Imhealthytoday (not shared and not accessible by anyone else).
- Both organizations (Educator-Resources & Imhealthytoday) are regulated by state authorities.
- The data is not shared or provided to any 3rd party in any manner other than listed above.
- If requested and required by law, data will be provided to government organizations.

Cybersecurity

IHT uses the Amazon Web Service encrypted file system where all data and metadata is encrypted at rest using an industry-standard AES-256 encryption algorithm. Encryption and decryption are handled automatically and transparently. We use encryption in transit using Transport Layer Security 1.2 (TLS, formerly called Secure Sockets Layer [SSL]) with an industry-standard AES-256 cipher. TLS is a set of industry-standard cryptographic protocols

used for encrypting information that is exchanged over the wire. AES-256 is a 256-bit encryption cipher used for data transmission in TLS. We employ Role Base Access Control (RBAC) grants access based on a user's role and implements key security principles, such as "least privilege" and "separation of privilege." Anyone attempting to access information can only access data that are deemed necessary for their role.

All personal data is processed, in compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH").