

A Note From...



The Children's School

emocha Health®

Dear TCS Parents,

To keep your children and our community safe, The Children's School is utilizing a digital health company, emocha, to monitor staff and students for symptoms of COVID-19.

Beginning on August 31st, we will use emocha's mobile app to enable parents on behalf of their students to conduct a self-screening of symptoms each day before reporting to school. All employees of TCS will also be asked to complete the screening process as well.

In order to roll-out this tool, TCS will share with very limited personal data. Data uploaded to emocha will include: student first and last names and parent cell phone numbers. [Click here to see emocha's full privacy policy.](#)

The emocha solution is HIPAA-compliant, meaning the data is secure and not shared with anyone outside of The Children's School -- we maintain strict confidentiality of all protected health information. Students and faculty will receive a color-coded digital badge through the mobile app to clear them to enter campus.

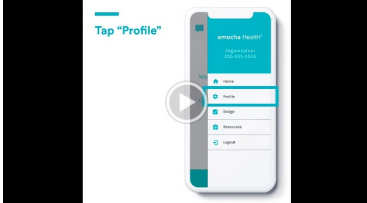
App users will receive a text message from emocha on **Wednesday, August 26th** that will help walk them through enrollment.

We ask that users respond to this text message and download the app within 24 hours, as the link will expire.

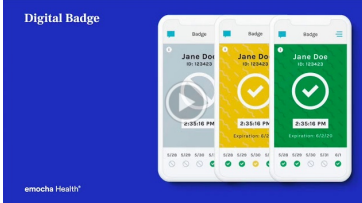
The emocha team will offer step-by-step instructions on the program, and our staff will be available to answer any of your questions. Please visit [this landing page](#) for additional information.

Thank you for your support as we begin to safely implement our return-to-campus plans. If you have any concerns regarding emocha screening, please feel free to reach out to Jesse Brand by email at jbrand@tcslj.org. As you begin using the program, if you need technical support, please contact emocha directly by calling (858)284-4120.

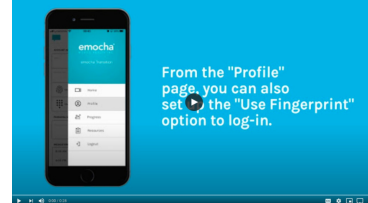
emocha Resources



Multiple Login Overview



Symptoms Monitoring Service for Students and Faculty



How to Set up a Pin

emocha Health

Remote Monitoring Service
for The Children's School

User Guide

www.emocha.com

helpdesk@emocha.com

[@emochahealth](https://twitter.com/emochahealth)

emocha Health User Guide

emocha Health

HIPAA-Compliance & Security

- The emocha platform is a suite of remote engagement and monitoring applications, with both mobile (iOS/ Android) and web components.
- emocha's technology was initially conceived by clinicians and public health scientists at Johns Hopkins University in 2006, making emocha one of the first mobile health platforms ever. All emocha applications comply with HIPAA regulations on how to handle protected health information (PHI), including – but not limited to – secure encryption of data, access controls, and industry-standard best practices.
- A robust & comprehensive role-based permission system limits system access to only authorized, authenticated users to ensure the need-to-know basis of PHI.
- All PHI is encrypted both in-flight and at rest, and all access to, or modification of, patient data and system configuration is logged, complying with HIPAA requirements.
- The server infrastructure is secured from both physical and remote access. emocha also requires that all providers of external information system services comply with security requirements related to PHI and HIPAA regulations.
- Data is stored for 7 years, per HIPAA requirements.

Information Storage

- emocha's servers are hosted "in the cloud" via Amazon Web Servers at secure data centers. Physical access is extremely limited, if not impossible.
- Log-in credentials are managed by a combination of strong password and private keys.

Password Protection

- emocha enforces specific identification and authentication procedures through password complexity, forcing users to change the default password at first login, and continuously working to ensure that all user accounts are unique.
- Additional criteria to ensure password protection includes a password-protected screen lock mechanism, and a session lock after 15 minutes of inactivity.

Encryption

emocha Health Inc. | 1818 N. Charles Street, 2nd floor | Suite 200, Baltimore, MD 21201 | info@emochahealth.com

Privacy & Security Talking Points

General Questions

Why am I being asked to participate in this program?
To keep your school community safe in response to the coronavirus pandemic, this program helps support students and staff in tracking any symptoms they may experience. Use of the emocha health app will allow us to regularly monitor students and staff for symptoms and ensure anyone entering campus is symptom-free.

Where can I go to get more information?
emocha provides a HIPAA secure e-way chat so that you can reach out to our Patient Solutions team. emocha can respond to questions submitted through this chat. In addition to this FAQ page, your school will provide additional resources to support community members in enrolling in emocha. Resources and contact information for each school are also listed in the emocha app Resources tab.

Is this mandatory?
Check with your school administrators for their specific policy on using emocha. Even if participation is not required, emocha is strongly recommended to help track symptoms in one system. emocha is designed to do this in a streamlined, simplified way for you and for your community.

How long is the program?
The monitoring period is typically 90 days, but will depend on your school's policies. emocha will let users know when their monitoring period is complete.

How can I access my test results?
emocha does not offer any information regarding testing results. To access results, please contact your testing facility or healthcare provider.

What do I do if there is an emergency?
You should dial 911 in case of emergency.

Which app do I download?
You should download the emocha asynchronous video DOT application from the Apple App Store or the Google Play Store.

Can I use the emocha app from any mobile device?
Yes. During enrollment, the phone number associated with the account will receive the welcome text message and prompt the recipient to download the app, create a password, and log in. These credentials can be used without any additional text enrollment from other phone numbers or devices.

My emocha account was created under an incorrect phone number. How can I change the phone number?

Frequently Asked Questions

emocha Health

HIPAA

HIPAA-Compliant
emocha requires that all providers of external information system services comply with security requirements related to Protected Health Information and HIPAA regulations. emocha additionally supports industry standard best practices for secure encryption of data, access controls, and 42 CFR Part 2 patient electronic consent requirements.

emocha can provide a Business Associates Agreement to employer customers, treating symptoms reports as medical data.

Password-Protected:
emocha enforces specific identification and authentication procedures through password complexity, forcing users to change the default password at first login, and working to ensure that all user accounts are unique. Additional criteria utilized to ensure password protection includes a password-protected screen lock mechanism, and a session lock after 15 minutes of inactivity.

emocha HIPAA Statement