

Summer Camp - My View & Tickit Health FAQ

Table of Contents

Intro	2
Who is Tickit Health?	
What is Tickit?	
What is Summer Camp - My View?	
FAQ: Summer Camp - My View	3
Setting up: How do I administer My View?	
Is the data provided by a camper linked to them personally or is it anonymous?	
Will we need extra devices to view results?	
When is camper data reviewed? What about critical issues?	
Troubleshooting	
FAQ: Tickit Health	4
About Tickit™	
Data Management	
Privacy & Security	

Intro

Who is Tickit Health?

For more than 10 years, Tickit Health has been used in children's hospitals and schools for MESH screening. The company was co-founded by pediatrician, Dr Sandy Whitehouse, and originally created to help young patients share their concerns with nurses and doctors.

Unlike traditional screening platforms, Tickit Health was co-designed with youth and developed in collaboration with global youth health leaders - incorporating a new design framework, Digital Empathy™ to revolutionize survey tools. The reporting of the data captured has been designed to improve workflow and efficiency. Schools using Tickit have reported a positive impact on improving youth engagement and connectedness. The platform data has helped staff identify and manage issues that were previously unknown.

We are excited to bring Tickit Health to camp.

What is Tickit?

Tickit is an evidence-based screening platform that provides a safe space for children (grade 4 and up) and youth to share important information about themselves.

The platform has two components:

- a web-based app that includes the My View screener. My View is easy-to-use and is accessed by a web link
- a password protected private and secure dashboard that displays the information collected in clear and simple reports and analytics

The platform can be integrated into other camp software and meets the highest privacy and security standards.

What is Summer Camp - My View?

"Summer Camp - My View" is a screening tool that can be administered before campers go to camp. Built on the principles of Digital Empathy™, My View is designed to be child and youth centered and strengths based to empower campers to feel safe and heard. Campers have an opportunity to share important information about their mental, emotional, and social health that could impact their stay at camp. It can be used by campers as young as 8-10 years old. Understanding the MESH profile of campers helps ensure a safe, healthy and fun camp experience.

The My View package includes a parent information handout for you to share with camper's parents.

FAQ: Summer Camp - My View

Getting started

What do I need?

With access to a desktop computer or laptop connected to wifi you will be able to administer My View and review the live results from your campers on the Tickit Health Dashboard.

Please note: In the following FAQs, the person who accesses the dashboard is called the *Camp Leader*. The *Camp Leader* will vary depending on how your organization is structured.

Setting up:

We understand that bringing new software to an organization can be daunting, and have focussed on making Tickit implementation, workflow and management straightforward and easy. **Onboarding to learn the software usually takes less than 30 minutes.**

You will get an email with credentials to Tickit Health for you to set up your account with your password. If you forget your password, you can use the "Forgot Password Feature" on the login screen to reset it. (<https://us.tickitforhealth.com/dashboard/login>)

How do I administer My View?

The suggested workflow to administer My View for this pilot project is to use a QR code printed on a poster for the camper or parent to use to get the link to the My View screener.

Tickit will provide you with a poster and specific QR code in PDF format for you to print and display.

Other ways you can send campers a link to My View:

- 1) Custom Links: To set up a link to My View that is tied to a specific camper and is sent directly to their device, first you can create a profile for the camper on the Tickit Health Dashboard.
- 2) Email Merge: Send a batch of links to My View via email to a list of campers. This can be done easily by using a free email merge service.

- 3) Using your registration software: To send links to My View directly from your registration software, the Tickit Health technical team will work with you to explore feasibility and functionality of this method.

Note: For all the above methods, you are able to send the link in advance of camp starting, at time of camper drop off, and/or after camp has begun provided there is internet access.

Is the data provided by a camper linked to them personally or is it anonymous?

There are lots of options to manage and keep private the information you receive.

- When campers open the link to My View, a unique link built into the system will provide their identification, so they don't have to put in any personal information. (Workflow dependent.)
- When you set up Tickit at your organization you can determine if the data is identifiable or anonymous depending on your needs.
- Access to the dashboard is password protected access. The Camp Director chooses who can access the data (the *Camp Leader*). Additional types of limited access roles to the data, for example for researchers, are available.
- Data can be downloaded for more detailed evaluation/analysis.

Will we need extra devices to view results?

Nope! Results for camper data/results can be accessed through a password protected site on the *Camp Leader's* work computer.

When is camper data reviewed? What about critical issues?

As soon as a camper completes My View, a report is generated under the camper's name. Notifications can be sent to the *Camp Leader* to inform them the data is available for review. For accountability, when the *Camp Leader* has reviewed the report, they can indicate that it is reviewed or approved on the report.

If there is a critical response, Tickit's alert system can be set-up to notify the *Camp Leader* by SMS or text.

Is any data stored on the devices themselves?

No! All data captured is stored on the private and secure Tickit® infrastructure.

Is any personally identifiable information or data shared with or sold to any third parties?

No! All personally identifiable information that is captured is limited in its accessibility to the organization that invited the respondent to submit the information, and no personally identifiable information is shared with or sold to any third parties (such as pharmaceutical or insurance company).

Troubleshooting:

It is rare that organizations require additional support once they are set up.

- There is a training link available Tickit Health demo for Summer Camp - My View for My View customers
- Troubleshooting:
 - link to a helpdesk via dashboard (Zendesk) with help articles
 - email questions and responses usually within 24 hours on weekdays, via dashboard or support@tickithealth.com
 - Office hours: designed to assist the onboarding phase

What if I forget my Dashboard password?

After your account is set up, you will receive a welcome email inviting you to sign in to the Tickit Health Dashboard by using your email address and creating a password. If you forget your password, you can use the “Forgot Password Feature” on the login screen to reset it.

<https://us.tickitforhealth.com/dashboard/login>

As a HIPPA compliant organization, all passwords are required to be a minimum of 10 characters with a mix of uppercase and lowercase, numerals, and special characters.

FAQ: Tickit Health

The following are frequently asked questions and answers regarding Tickit®, its architecture, and the privacy & security of the data entrusted to it. While we are unable to generally share specific architectural details for reasons of security, if further information is required, please contact us.

What other tools are available on Tickit?

There are many tools available on the Tickit platform, including validated surveys, Patient Reported Experience Measures, Patient Reported Outcome Measures. We also have patient education and patient decision making tools. Please contact us to obtain our Tickit Tool Library.



What languages are supported on Tickit?

The Tickit user interface supports any language, any script, including languages that are read right to left. The dashboard is in English.

Can new surveys/assessments be added to Tickit?

We pride ourselves in working in collaboration with our clients and applying design thinking and patient centric design to create new tools.

Which devices are supported by Tickit?

- Tickit® works with any device.
- Tickit® is responsive and resizes any screener so the user experience is amazing and seamless regardless of screen size or type of device.
- Tickit's design and content is developed for accessibility (WCAG 2.0 compliant) and utilized for vulnerable populations with visual impairments and low literacy.
- Tickit® works with all modern browsers. Below is the compatibility with different browsers.

Browser Name	Survey Compatible	Dashboard Compatible
Opera	25+	25+
Mozilla Firefox	30+	30+
Google Chrome	42+	42+
Internet Explorer	Not supported	11+
Microsoft Edge	Blocked	13+
Apple Safari	9+ (9.3.3/ios 9+ for attract loop)	9+

DATA MANAGEMENT

Can the data from Tickit be downloaded and/or integrated with other 3rd party systems?

The data collected on the Tickit platform is owned by the organization that has the license, It is not shared with any third party, nor accessed by Tickit Health staff.

Licensed and authorized organizations and their users can download their specific data (as controlled by their authorization privileges).



If a licensed organization, Tickit® enables several alternatives for integration and inter-operation with other operational systems such as Electronic Health/Medical Record systems, Learning Management Systems, and CRM systems.

Tickit has an API that can connect with Electronic Health Records. However this is not an automatic function. Reports and survey results may be converted to PDF or attached in printed form to records by clinic staff if desired. Please contact us to discuss your interoperability needs.

Where is the data stored?

All personally identifiable data is stored in the country in which it is captured, in best-in-class secured data centers. Data centres themselves adhere to security controls for ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP and ENS

Can Tickit Health's team see any personally identifiable information?

Generally, No. Only Super-Administrators have the ability to access source data for purposes of technical troubleshooting and access traceability. However, licensed organizations have the ability to hide the respondent identifiers from Tickit Health.. In doing so, we store only an arbitrary but unique reference key to the real identifier

An individual's identity and data can only be accessed and viewed by the Tickit® user-role granted the proper access credentials by the organization who gave them authority to use Tickit.

FAQ: PRIVACY & SECURITY

Is Tickit® Health compliant with applicable privacy and security laws?

Yes. Tickit® Health has established a comprehensive Information Privacy and Security Management Program (IPSMP). This program conforms to the principles outlined in ISO/IEC 27002:2013 - Code of practice for information security controls, and others, including:

- Health Insurance Portability and Accountability Act (HIPAA)
- Personal Health Information Protection Act (PHIPA)
- Freedom of Information and Privacy Protection Act of British Columbia (FOIPPA)
- Personal Information Protection and Electronic Documents Act of Canada (PIPEDA)
- Canadian Standards Association (CSA) Model Code for the Protection of Personal Information
- Information Privacy Act of Australia (2009)

What other actions or efforts has Tickit Health made to ensure privacy & security of personally identifiable information?

Tickit® Health has appointed a Chief Privacy and Security Officer to oversee all aspects of the IPSMP.

Tickit® Health routinely conducts – in conjunction with a 3rd party reviewer - Privacy Impact Assessments (PIAs) and Security Threat and Risk Assessments (TRAs) on the Tickit® platform. Risk treatment plans are established to ensure that privacy and security risks are addressed and remain at tolerable levels. PIA and TRA summaries are available to Tickit® Health customers on request and under Non-Disclosure.

All Tickit® Health staff and agents have signed confidentiality agreements, acceptable use agreements, and have received privacy and security awareness training; such training repeated at least annually.

- Tickit® Health maintains comprehensive privacy and security policies.
- Tickit® Health maintains a security penetration testing and vulnerability assessment program to confirm that adequate safeguards are in place. The testing is conducted by 3rd parties.
- Tickit® Health has established privacy and security incident management protocols to identify, contain and manage privacy and security breaches.
- The Tickit® technology itself applies the following physical and technical safeguards:
 - Application and backup are housed in secure data centres located in the country of data origin
 - Data centres themselves adhere to security controls for ISO 27001, ISO 27018, SOC 1, SOC 2, SOC3, FedRAMP, HITRUST, MTCS, IRAP and ENS
 - Passwords are hashed with a per-user salt. No-one (besides the user) knows the user's password.
 - Role-based access control
 - Data is encrypted in transit and at-rest
 - Auto log off after a defined period of time
 - Audit logs are maintained in-definitely
 - Input integrity controls
 - Password strength requirements
 - Login/ password authentication and authorization for licensees
 - Two-factor authentication for Tickit® Health Staff
 - Automatic backups
 - Least privilege principle