Well-Being Index Technical/Security Whitepaper

Vendor Contact Information

Vendor Name:	Corporate Web Services, Inc. (dba: MedEd Web Solutions)
Vendor EIN:	87-0572828
Vendor Contact Name:	Alan De Keyrel
Vendor Contact Email:	alan@mywellbeingindex.org
Vendor Contact Phone:	507.289.2229 x704
Vendor/Product URL:	https://mywellbeingindex.org
Product Name:	Well-Being Index
Application URL:	https://app.mywellbeingindex.org

Product Overview

Provide an overview of the application and how it is used

- The Well-Being Index is an online self-assessment tool invented by Mayo Clinic that measures six dimensions of distress and well-being in just nine questions. The Well-Being Index equips organizations with the data and tools needed to go beyond burnout while providing participants with customized resources, internal and national benchmarking, options for feedback, and complete anonymity. Current versions include physician, resident & fellow, medical student, nurse, advanced practice provider, and employee. Our mission is to improve well-being among professionals and eliminate the adverse consequences that are associated with distress. You can assess your own well-being by downloading the mobile app for Apple iOS or Android phones. You can demo the full application at https://demo.mywellbeingindex.org/.

What are the primary customer interfaces for the app?

- The app is entirely web-based and provided as a service (SAAS). The only requirement for participation is internet access to the assessment website with a modern web browser. We support desktop and mobile views on Internet Explorer 10+, Chrome, Safari, and Firefox, and our smartphone app is available for download.

What information feeds and/or integrations does our institution need to provide?

- None, all data is supplied by users. The Well-Being Index is purposefully not integrated with your institutional infrastructure to maintain participant anonymity.

What server, workstation, mobile platforms and operating systems are required for the app?

- Since the solution is provided as Software As A Service (SAAS), no hardware is required from your organization. The only requirement is that participants have an Internet connected device with a modern web browser (Internet Explorer 10+, Chrome, Safari, and Firefox), or a smartphone to use the app.
- The iOS or Android app can optionally be used to access the Well-Being Index. The mobile app can be downloaded from the Apple App Store or Google Play store.

Does the app use any third party software plugins?

- The app will utilize jQuery, jQuery UI, Google Charts (JS API), and Google Tag Manager.

Hosting

Is this a hosted platform?

- This is a vendor-hosted application and provided to you as a web-based app in a traditional SAAS model.

Is the hosting facility owned by the vendor or contracted by a third company?

- Hosting infrastructure for the app is with a secured third party private cloud provider.

Security

Does the solution store Personal Identifiable Information including HIPAA and PCI?

- The app collects a user's email address, password, and demographic data such as age, specialty, and gender. After answering the questions, a proprietary Well-Being score is assigned and stored to track well-being over time. The participant can optionally provide a cell phone number for periodic reminders. All of the data collected by the app is non-PHI as deemed by Mayo Clinic.

How does the solution encrypt and protect data in transit and at rest?

- All app pages are loaded over a TLS encrypted connection. Data at-rest is stored as AES encrypted and salted database column.
- Least-privilege firewall and ACL rules protect the various hosted network segments.
- The database is hosted as a separate entity and only internal connections from the web hosts are allowed.

How is access to data logged, and is this autited?

- Data access attempts are logged internally. Data access privileges and log files are reviewed regularly.

How are users provisioned and managed?

- Your institution will invite individuals to participate in the Well-Being Index by providing them a unique invitation code. They are then able to complete the signup process by using any email address as their login and a strong password (passwords must be at least 8 characters and not be common or dictionary words). We do not use SAML, single-sign-on, etc., this is done in order to keep the user data de-identifiable.

Can data be exported by the end-user? If so, describe the process and format?

- Institutional administrators can export de-identified aggregate reports as a PDF file.

How long does the app retain data?

- We retain all participant data (account information, scores, etc) indefinitely to track their well-being over time. System data is backed up regularly, and these backups are retained for a period of time.

What firewall ports need to be opened by our institution for the app to function?

- Nothing nonstandard. Participants only access https://app.mywellbeingindex.org via a web browser; so, their browser needs the ability to resolve public DNS (port 53) and to communicate over HTTPS (port 443).

Who has access to the data?

- In order to maintain participant anonymity, your institutional administrators will only be provided data/reports in de-identified aggregate form. Only specific Vendor personnel have direct access to the database data and authorization is solely granted for the purpose of maintaining the data within the app.

When was the last I.S. Security audit completed? Can you provide the results?

- We have a current information security review/audit contract with a qualified third party, that includes security program gap analysis, improvement, and concludes with a comprehensive annual audit of our NIST & ISO standardized security practices. Improving the security of our infrastructure is a regular and ongoing process, therefore we do not share the results of any given report with outside parties. If requested, we can provide you with a letter of engagement from our third party security vendor.
- We perform vulnerability and penetration testing on the app quarterly.

Will you sign a BAA or FERPA with us?

- Since the data collected has been deemed non-PHI by Mayo Clinic, a Business Associate Agreement (BAA) is not necessary for HIPAA compliance. However, if your organization involves medical students we are willing to sign a standard FERPA. Please send FERPA requests to the Vendor Contact Email at the top of this document.

Can our institution do a full security review before we sign up?

- We're trying to keep the Well-Being Index affordable, so that means we don't have the ability to meet with every security team and do a full security audit. Hopefully this whitepaper meets your needs for vetting whether the WBI (Invented by Mayo Clinic) works for your organization. If not, we'd be happy to discuss charges you may incur for a full security review. Additional questions not answered can be sent to the Vendor Contact Email listed at the top of the document.

Support Model

Describe the support model for the product?

- The Well-Being Index is provided as Software As A Services (SAAS), therefore, all support is provided by the Vendor.

What are the support escalation paths for the product?

- Vendor has support escalation procedures in place. In most support situations, your institutional IT support services are not needed.

What is the SLA for the product?

- Our standard SAAS/License agreement specifies SLA details. Uptime/availability is guaranteed for 99.8% of the time excluding scheduled maintenance.

Authentication/Password Requirements

Does the “reset your password” feature expire or have a one-time use?

- The password reset link does not expire but it is only valid for a one-time password reset.

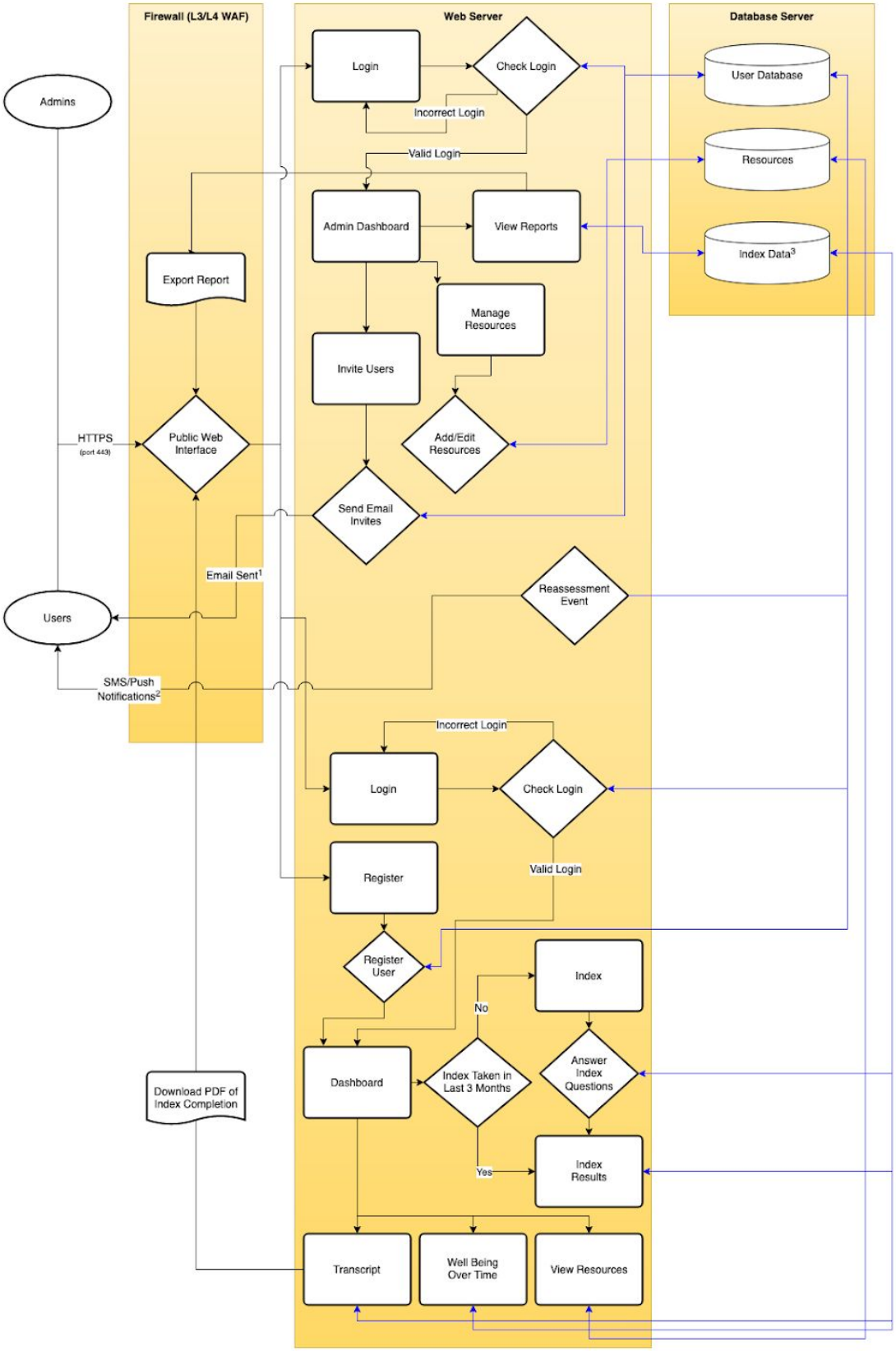
How often do you require them to change their password?

- There is no password expiration. This is done because most users will not be frequently logging into the app, and having them change their strong password every time they login would deter many from continually assessing their well-being. We hope to be a solution to distress, not a contributing factor.

Do you offer 2 factor authentication?

- To reduce frustration and increase reassessment of users we do not require 2 factor authentication. Multi-step login would deter users from using the app and they would give up, and this would not help them or your institution. Mayo Clinic has decided a common-sense approach to security based on data that is being collected makes sense.

Data Flow Diagram



[1]Email messages are sent through a cloud SMTP email service.

[2]SMS text message reminders are sent through Twilio, and Push Notifications are sent through Apple and Android services to users' mobile phones.

[3]Users' answers to the index questions are stored encrypted with AES before they are saved to the database.

Infrastructure Diagram