Well-Being Index

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@mededwebs.com
Vendor Contact Phone:	507.289.2229 x704
Vendor/Product URL:	https://www.mededwebs.com/well-being-index
Product Name:	Physician Well-Being Index
Application URL:	https://mywellbeingindex.org

Product Overview

Provide an overview of the application and how it is used

- The Well-Being Index was invented by the Mayo Clinic to address the problem of physician burnout and distress. The WBI is a 100% anonymous, web-based self-assessment tool that evaluates multiple dimensions of distress in just 9 questions. The Well-Being Index promotes self-awareness by measuring burnout/distress, providing valuable resources when physicians need them most and tracks their well-being over time. Our missions is to reduce burnout among healthcare professionals and eliminate the adverse consequences that are associated with distressed workers. You can assess your own well-being and/or demo the tool at https://www.mywellbeingindex.org/assess.

Describe the primary customer interfaces for the application.

- The software is entirely web-based and provided as a service (SAAS). The only requirement for physician 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.

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 application?

- 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).

What database platform does the product leverage?

- MySQL

What programming languages are used in the application?

- PHP, HTML5

Does the solution use any third party plugins?

- None that would need to be installed by the participant. We 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 service.

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

- The secure hosting facility is owned and operated by the vendor (Corporate Web Services) in our Rochester, MN datacenter.

What type of physical security controls are in place for Vendor's servers?

- Key-card access & logging to perimeter doors.
- Key-card access & logging to server room door.
- Video Surveillance & Recording of the facility and server room.
- Onsite power generator capable of providing off-grid power for days.

What type of technical controls are in place for protecting data at the hosting provider?

- Web server and database server are separate platforms, and full network segmentation and firewall exists between them.
- Advanced firewall protection at all network layers for web service interfaces, including Web Application Firewall & SPI.
- Administrative access to hosting components is limited to only authenticated vendor employees while onsite or on secured VPN.

List the vendor and version for the following components leveraged in your hosted environment.

- VPN: Sophos UTM v9

- IPS: Sophos UTM v9
- IDS: Sophos UTM v9
- DLP: None
- Virus Scanning: inline HTTP request scanning: Sophos UTM v9
- Device Encryption: None (except database column encryption mentioned below)
- Two Factor Auth: Not Used (Described below)
- Firewall: Sophos UTM v9 Stateful L3 firewall.

Security

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

- The web-based software collects a user's email address, password and demographic data such as age, specialty, and gender. After answering the 9 questions, a proprietary Well-Being score is assigned and store 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 software is non-PHI as deemed by Mayo Clinic.

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

- All application pages are loaded over a TLS encrypted connection. Data at-rest is stored as AES encrypted and salted database column. The hosting servers are protected by redundant Sophos firewalls. The web application is protected by redundant Sophos firewalls. The firewalls will only allow web-based traffic onto the Web Server and also detects and blocks malicious web traffic.
- The database is located on a separate server and only internal connections are allowed. The web server will connect to save and retrieve data for the Well-Being Index application. All sensitive data is encrypted using 256 bit AES encryption before storage within the database.

How is access to data logged?

- All login attempts to the server are saved to an internal system log.

How are users provisioned and managed?

- Your institution will invite physicians 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 long and must contain at least one lowercase letter, uppercase letter, number, and symbol). We do not use SAML, single-sign-on, etc 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.

What are the products data retention requirements?

- We retain all participant data (account information, scores, etc) indefinitely to track their well-being over time. System data is backed up regularly, and backup stores are retained for 7 days.

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

- Nothing nonstandard. Participants only access https://*.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 the Vendor has database access to identifiable data and authorization is solely granted for the purpose of maintaining the application.

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 (and satisfying HIPAA hosting rules). 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.

Will you sign a BAA or FERPA with us?

- Since the data collected has been deemed non-PHI by the 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. Institutional IT support services are not needed.

What is the SLA for the product?

- Our standard SAAS/License agreement guarantees the application will be available 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 software, 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 the burnout problem, 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 software 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. All of the data collected by the software is non-PHI as deemed by Mayo Clinic.