

**INSTRUCTIONS FOR USE (IFU)**

**WEA**<sup>TM</sup>  
**Portal**

SUMMARY

- 1 Introduction .....4
  - 1.1 Intended Use.....4
  - 1.2 Target Population.....4
  - 1.3 Compatibility with Other Medical Devices .....4
  - 1.4 Precautions for Use .....4
  - 1.5 Contraindications .....4
- 2 Minimum Required Configurations .....5
  - 2.1 Minimal Configuration Advised .....5
  - 2.2 Screen Resolution.....5
  - 2.3 Internet Configuration .....5
  - 2.4 Web Browser Cache .....5
- 3 Security Recommendations.....6
  - 3.1 User Credentials .....6
  - 3.2 User Environment .....6
  - 3.3 User Access.....6
  - 3.4 Application’s Servers .....7
  - 3.5 Information to the User .....7
  - 3.6 Report a Cybersecurity Incident .....7
- 4 Product Information .....8
- 5 Contact Us.....9
- 6 Appendix 1: Clearing your Browser Cache .....10

The software, acquired under license, is protected by legislation on industrial and intellectual property in its country of origin, in accordance with French and European legislation, as well as by application of international agreements on the matter.

Except as expressly permitted by EOS imaging with a prior written consent, user will not, and will not allow others to:

- Remove any copyright, trade secret, or other proprietary right notices contained on or in the Software or Documentation as provided by EOS imaging.
- Reproduce or modify any Software or Documentation or copy of all or any part of either.
- Reverse assemble, reverse engineer, or decompile any Software or copy of all or any part of the Software, in whole or in part (except as provided by applicable law).
- Sell, transfer, or otherwise make available to any third party the Software or Documentation, or any copy of all or any part of either.

Any person failing to respect these provisions will be guilty of infringement punishable by criminal law.

**NOTE**

Any personal data appearing in the screen captures of this document is fictional.

**NOTE**

Alphatec Spine (ATEC) is referenced within this document. ATEC is the parent company of EOS imaging.


Copyright © 2023 EOS imaging

## 1 Introduction

This software, available online, is a platform designed for the management of orthopedic operations handled via the dedicated preoperative planning process. It is available at the following addresses:

- <https://www.vea-align.atecspine.com/> from the United States.

The latest version of software Instructions for Use (IFU) is available in electronic format from the software interface.

The  button enables access to the page listing these documents.

The functions of the VEA Portal are described in a dedicated user manual. The user manual is available upon request.

### 1.1 Intended Use

VEA Portal is an online digital platform that provides Physicians centralized access to software applications.

### 1.2 Target Population

VEA Portal is an online digital platform which does not affect any patient.

### 1.3 Compatibility with Other Medical Devices

VEA Portal provides access to VEA Align software.

### 1.4 Precautions for Use



#### **IMPORTANT**

Read the Instructions for Use (IFU) carefully before using.

### 1.5 Contraindications

VEA Portal has no contraindications.

## 2 Minimum Required Configurations

Not intended for use on mobile devices.

### 2.1 Minimal Configuration Advised

- A stable internet connection is required (see part “2.3 Internet ”).
- With Windows 10 or 11: Google Chrome in version 112 or higher, and Edge in version 112 or higher.
- With Mac OS Monterey or Ventura: Google Chrome in version 112 or higher.

It is the user's responsibility to keep his/her web browser up to date for a better functioning of the software.

### 2.2 Screen Resolution

The minimum screen resolution ensuring full display of the interface is 1366 x 768.

#### NOTE

HD screens are compatible with the application.

### 2.3 Internet Configuration

A stable high-speed internet connection is required: DSL 100Mb/s connection or higher, Wi-Fi or Ethernet.

#### NOTE

Other connections such as a 5G/4G/3G connection can be used, but they must be stable. The user may then experience a relatively long load time for the software.

### 2.4 Web Browser Cache

When a new version of the software is deployed, it is strongly recommended that the web browser cache be emptied. The part “6 Appendix 1: Clearing your Browser ” explains how to perform this operation.

### 3 Security Recommendations

The use of the products does not require any additional software on the user's computer except an up-to-date web browser.

The product provides access to sensitive patient health information (PHI), and user should be mindful while using the product. The user is responsible for the security aspects of his computer.

The following section provides common recommendations about security on the web that applies to the product's use.

#### 3.1 User Credentials

The product requires users to login before accessing any data or resources.

Each user has a unique account created when purchasing the product. Accounts and credentials shall not be shared among multiple users.

The product uses the following security measures to protect accounts:

- User must define strong password:
  - The size of the password must be between 8 and 72 characters included 3 out of the 4 below:
    - Has at least one uppercase
    - Has at least one lowercase
    - Has at least one number
    - Has at least one symbol
- Accounts use multi-factor authentication:
  - The user identity is verified by sending a message, or notification, to the phone when attempting to login.
  - The phone number is defined when creating an account.

A TEC and EOS employees do not have access to your password, and in any event, would never ask you to provide your password.

If this happens, contact immediately your ATEC/EOS representative, or use the contact information available in §5 Contact

#### 3.2 User Environment

The use of a modern, auto-updated, browser is recommended.

The user must respect the common recommendations about security on the web:

- Apply security updates to the user's computer as soon as they are available
- Use antivirus software on the user's computer
- Download applications only from official websites
- Don't diffuse any information, especially about application's access and patient data on social networks
- Separate personal and professional uses
- Avoid public or unknown Wi-Fi networks

#### 3.3 User Access

The product implements HTTPS protocol for communication between the user's web browser and the application's server. The protocol encrypts end-to-end communication to ensure confidentiality, and integrity, of information.

The user must respect the common recommendations about security on the web:

- Use only the address <https://www.vea-align.atecspine.com> to access the application
- Make sure that the connection uses HTTPS protocol to access the application
- Log out from the application after each use

A TEC and EOS products use a trusted certificate authority to enable https. If your browser notifies an untrusted certificate when using the product, close your browser and contact immediately your ATEC/EOS representative, or use the contact information available in §5 Contact .

### 3.4 Application's Servers

The product is a web application hosted and deployed on a datacenter certified for hosting Patient Health Information and is HIPAA compliant.

The main feature of the server is to protect personal health information. The server is installed in an environment that complies with the standards in force for this type of use. Moreover, the https protocol is used to connect to it, thus ensuring data transfer security.

Server's security is under the responsibility of the manufacturer.

### 3.5 Information to the User

The deployment of a new version of the device is followed by an information to the user on what updates have been performed on the device. The user has directly access to the last version of the device is a web application.

If a cybersecurity vulnerability or event is detected on the device, depending on its severity and impact on the user, a communication is performed with details on vulnerabilities and recommendations.

### 3.6 Report a Cybersecurity Incident

If you believe a potential security vulnerability occurs in one of our products or services, please contact us immediately. Contact details are available at §5 Contact .





So, we can proceed to proper investigation and initiate corrections as soon as possible, please provide at least the following:

- Contact details (name and address of the site, contact person name, function, phone number and email address)
- Product impacted (Model and serial number)
- Date and time of incident
- Any error message that has appeared
- Any action made by the user before and after the security vulnerability was suspected
- Any other event or source from which the security vulnerability is suspected to come from
- Any additional information you judge necessary to understand and investigate the event

## 4 Product Information

Information for product identification is available from the about page of the software.

The following symbols are used on this page:

Symbol	Meaning
	Medical device
	Unique Device Identifier
	Manufacturer
	Consult the provided documentation
<b>Rx only</b>	Valid for the United States: Caution: Federal law restricts these devices to sale by or on the order of a physician.




## 5 Contact Us

For any questions or assistance, contact the Technical Support of VEA Portal:


- Email: [help-vea@atecspine.com](mailto:help-vea@atecspine.com)
- Website: <https://www.atecspine.com>

## 6 Appendix 1: Clearing your Browser Cache

### Google Chrome:

- In Chrome, at the top right, click .
- Click on “More tools” then “Delete browsing data”.
- At the top of the page, choose “All time” in the “Time range” drop down list.
- Check the boxes “Cookies and website data” and “Cached images and files”.
- Click on “Delete Data”.
- Close the page.

### Edge:

- In Edge, at the top right, click .
- Click on “Settings” then “Privacy, search and services” in the left panel
- In the part “Clear browsing data” click on the button “Choose what to clear”.
- At the top of the page, choose “All time” in the “Time range” drop down list.
- Check the boxes “Cookies and other site data” and “Cached images and files”.
- Click on “Clear now”.
- Close the page.