

AllegianceMD Software Inc.

6914 S. Yorktown Ave., Suite 200 Tulsa, OK 74136
Phone: 800-868-1923 www.allegiancemd.com

Costs Of Certified Health IT

Developer: AllegianceMD Software Inc.

Product: Veracity **Version:** 9.1

Certified Product Information

URL: <https://chpl.healthit.gov/#/listing/10794>

Certificate Number: 15.02.05.2672.ALLE.01.01.1.220117

Certification Date: 01/17/2022

Additional Software: PHIMail, MyPortal.MD

Criteria Certified

170.315 (a)(1)	170.315 (c)(1)	170.315 (d)(13) – Cures
170.315 (a)(2)	170.315 (c)(2)	170.315 (e)(1) – Cures
170.315 (a)(3)	170.315 (c)(3) – Cures	170.315 (e)(3)
170.315 (a)(4)	170.315 (d)(1)	170.315 (f)(1)
170.315 (a)(5)	170.315 (d)(2) – Cures	170.315 (f)(5) – Cures
170.315 (a)(9)	170.315 (d)(3) – Cures	170.315 (g)(2)
170.315 (a)(12)	170.315 (d)(4)	170.315 (g)(3)
170.315 (a)(14)	170.315 (d)(5)	170.315 (g)(4)
170.315 (a)(15)	170.315 (d)(6)	170.315 (g)(5)
170.315 (b)(1) – Cures	170.315 (d)(7)	170.315 (g)(6) – Cures
170.315 (b)(2) – Cures	170.315 (d)(8)	170.315 (g)(7)
170.315 (b)(3) – Cures	170.315 (d)(9)	170.315 (g)(9) – Cures
170.315 (b)(10)	170.315 (d)(12) – Cures	170.315 (g)(10) – Cures
		170.315 (h)(1)

CQMs certified

CMS117v7, CMS122v7, CMS123v7, CMS124v7, CMS125v7, CMS127v7, CMS128v7, CMS129v8, CMS130v7, CMS131v7, CMS132v7, CMS133v7, CMS134v7, CMS135v7, CMS136v8, CMS137v7, CMS138v7, CMS139v7, CMS142v7, CMS143v7, CMS144v7, CMS145v7, CMS146v7, CMS147v8, CMS149v7, CMS153v7, CMS154v7, CMS155v7, CMS156v7, CMS157v7, CMS158v7, CMS159v7, CMS160v7, CMS161v7, CMS164v7, CMS165v7, CMS167v7, CMS177v7, CMS22v7, CMS249v1, CMS2v8, CMS349v1, CMS50v7, CMS52v7, CMS56v7, CMS645v2, CMS65v8, CMS66v7, CMS68v8, CMS69v7, CMS74v8, CMS75v7, CMS82v6, CMS90v8

The above product and version, Veracity 9.1, as certified has two (2) standard costs that are required to be paid by the practice/provider for the standard use of the program. These standard costs are as follow:

- A One time initial setup fee.
- A Monthly per provider subscription fee.

These two (2) standard fees cover the standard use of the Veracity 9.1 EMR system.

Disclaimer

This Health IT Module is 2015 Edition compliant and has been certified by an ONC-ACB in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services.

Additional Costs

Additional costs that may be encountered with the use of the AllegianceMD Veracity 9.1 EMR program in order to meet the certified objectives and measures outside of the standard initial set up fee and monthly per provider subscription fee that AllegianceMD Software Inc. charges are as follows:

- Interfaces to/with the following may require a one-time interface fee and/or annual maintenance/licensing fee that is charged by a 3rd party entity.
 - Interfaces with immunization registries.
 - Interfaces with laboratories and imaging centers.
 - Interfaces with health registries.
 - Interfaces with health information exchanges (HIE's).
 - Interfaces with public health agencies.
 - Interfaces with other health information services providers (HISP's).
 - Integration with other ONC certified systems.
 - Cost per patient export for Mass CCDA export of 10 cents/patient. Individual CCDA export is at no charge.
 - PHIMail is used to meet the direct protocol requirements of 170.315(B)(1), 170.315(H)(1).
- And the following - Only applicable for providers that will be e-prescribing controlled substances.
 - The mandated knowledge-based identification process required for EPCS set up entails an additional biennial fee that is good for 2 years and then is up for renewal every 2 years. This fee is also charged by a 3rd party entity.

Third Party Software

- PHIMail is used to meet the direct protocol requirements of 170.315(B)(1), 170.315(H)(1)
- MyPortal.md is used to meet 170.315(E)(1). myportal.md is owned and operated by AllegianceMD Software, Inc.

Two Factor Authentication 170.315(d)(13)

AllegianceMD offers free 2FA as an optional free of charge service. It works by the user enabling 2FA on their personal account. The user is then prompted to use authenticator app to scan a uniquely generated QR code. An example of an authenticator app, is Google Authenticator.

The user can use the authenticator app or email to get a one-time code. The one-time code is used in conjunction with username and password to successfully login.