ATTN: Drummond Group, LLC
3622 Lyckan Parkway, Suite 3003
Durham, NC 27707

July 15, 2024
Medisolv, Inc.
Product: Encor-E Version 6

To Drummond Group:

The Mandatory Disclosure statement of costs and any additional transparency information for our certified product(s) is attached to this letter and will be posted along with the required product information on our website here:

https://medisolv.com/certifications

We agree to notify Drummond Group of all future changes to our transparency and disclosures language for this certified product-version.

We understand and agree that the ONC Health IT Certification Program Final Rule statement gives Drummond Group, as an ONC-ACB, the sole responsibility for ensuring compliance and determining appropriate consequences if EHR technology developers fail to divulge accurate transparency and disclosures information.

We understand and agree that we will provide to Drummond Group copies of or give access to all websites, marketing materials, communication statements, and other assertions made by your organization regarding the ONC certification status of this product in a reasonable time to ensure the transparency and disclosures information is being accurately disclosed.

Justin Di Stefano

Justin S. Di Stefano
Vice President, Engineering
jdistefano@medisolv.com
(443) 264-4259

Costs

This certified product requires a one-time implementation cost and an annual subscription cost. The implementation cost is based on the number of product instances and data sources needed for setup. The subscription cost for hospital reporting is calculated per facility. For ambulatory reporting, the subscription cost is based on the number of clinicians the client has enabled for reporting.

Additional costs may be incurred if the client incorporates additional modules and/or needs custom data integration services. These services are needed when the data elements required to calculate certain measures are in other EMR systems (not previously integrated) or in non-standard locations within an EMR system.

Technical Details

This certified product-version may require the use of a virtual machine (or equivalent) on the client network to enable secure data transmission between the client EMR and the vendor's system. This may result in additional client costs associated with licensing the operating system and other necessary requirements, such as antivirus protection.

170.315(d)(12) and 170.315(d)(13) require the use of a properly setup client directory server. Encryption and multi-factor authentication (MFA) support is fully available via the use of either Microsoft Entra, Microsoft Azure Entra B2C, or SAML/SSO bindings to client directory systems. Medisolv offers MFA when using Microsoft Azure Entra B2C (upon client request, not enabled by default), and that support requires the use of a cell phone by end-users to receive the token(s). When using Microsoft Entra or SSO/SAML, encryption and MFA are optionally supported. Support requires that the client/hosting entity configures their directory system for both encryption and MFA.

Multi-Factor-Authentication Use-Cases

This certified product supports optional MFA for all user classes, roles, and application access if requested (for Azure Entra B2C), or if implemented by the client in the client's directory services (for Microsoft Entra or SSO/SAML).

In Azure Entra B2C, MFA is managed during centralized login and authentication. It is not applied on a per-user basis, meaning that MFA is either enabled or disabled for all users within a single instance of the software product.

In the context of SSO/SAML and Microsoft Entra, the client/directory-control officer has the authority to determine how MFA is implemented. SSO/SAML and Microsoft Entra use the client directory setup, including all MFA and encryption options. At the client's discretion, these settings can be segregated on a per-user basis. The software product does not make any decisions regarding MFA in an SSO/SAML and Microsoft Entra environment. Consequently, the directory-controller maintains complete control over who, how often, and in what manner MFA is applied during user authentication.