Cerner Corporation Certified Health IT Costs Information

Cerner is proud to offer products that are certified under the Office of the National Coordinator (ONC) for Health Information Technology's Health IT Certification Program. Contained within is a comprehensive list of Cerner certified Health IT Modules, the respective offerings, types of cost information, and significant implementation guidance for each.

To obtain more information about how Cerner products meet the ONC certification criteria and standards, please email us at ocregulatorycompliance_us@oracle.com. For unique certification numbers and test reports, please see ONCs Certified Health IT Product List.

Products listed within may incur varying degrees of costs related to professional services to support new implementations and upgrades depending on the election of the client under their contractual agreement with Cerner. Please note that in cases of upgrading code levels related to the applicable certified products, there may be optional implementation costs associated to adopt new features upon upgrade. Additionally, while professional services for upgrades are not generally required, they can help ensure questions related to adoption of new features are appropriately responded to and implementation of content and functionality better considers intended use.

NOTE: For clients using Cerner's CommunityWorks, Ambulatory Application Service Provider (ASP), or Integrated Behavioral Health services to support use of Cerner's certified products and who rely on Cerner to provide application and system management support on an outsourced basis as part of these offerings, reference to "Client" within this disclosure can mean user roles directly supported by Cerner associates acting in their capacity to provide application management services covered by such offerings. As a part of the outsourcing, clients should expect services to include managed IT infrastructure, system operations management and reference database configuration change management. Certain third-party software costs are included in the cost of these services. Any requests for services that fall outside the scope of the managed services offering will need to be evaluated for additional service fees.

It should also be noted that configuration of interfaces, exports or outputs of clinical documents or data that goes beyond the specifications, standards or requirements tested by certification are considered outside the CommunityWorks, Ambulatory ASP, and Integrated Behavioral Health offerings. Any such request that involves use of advanced qualification parameters, modification of standard reporting programs or interfaces to be adapted for other purposes are considered beyond the intended use of the certified capabilities and are subject to a fee.

Table of Contents

Millennium Certified Health IT Modules

Antimicrobial Usage and Resistance Reporting *See* Appendix A *for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique user identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: Cerner Millennium	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP).	Configuration of Millennium Core Security for user account security privileges, authentication parameters, and related access controls is required for use of the certified capability. As a part of standard implementation, defining and administering users, security roles, authorization and authentication parameters, and the like is required. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities, but are not incompatible with their use.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of access to ePHI via Antimicrobial Use (AU) and Antimicrobial Resistance (AR) report execution, including integrity protection of recorded audit logs. **Relied upon software**: Cerner Millennium, ntpd (Linux)	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP). Optional costs include the P2Sentinel Listener to enable audit events to be sent from the Millennium platform on which the certified product operates to an external third-party audit reporting application. Additional services-related costs may apply for configuration of outbound audit event data to meet the formatting constraints of any such third-party audit reporting application.	Configuration of the Millennium Core Audit Service, including enabling of desired audit events for logging and hash algorithm for tamper detection of captured audit data, must be completed for use of the certified capabilities. If a third-party audit reporting application is used, configuration of audit events to be securely transmitted from Millennium is required. Audit event data is captured and transmitted outbound to the audit log repository in XML format according to the Audit Trail and Node Authentication (ATNA) profile standard message structure and may be subject to customization or modification to conform to the inbound formatting requirements of any such third-party application.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. **Relied upon software**: ntpd (Linux)	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP). Use of *P2Sentinel* as the audit repository and reporting application is recommended and is subject to additional licensing costs. If a certified third-party audit reporting application (e.g., Fair Warning) is used in place of *P2Sentinel*, a license for the P2Sentinel Listener is recommended (but not required).	Reporting capabilities for audit events and data from the certified product that are captured via Millennium Core Audit Service require use of an external audit repository and reporting application to which audit data is securely transmitted after capture supporting physical separation of the audit log from the HIT module that is the subject of the audit in accordance with good security practices. *P2Sentinel* is recommended as the audit reporting application, but third-party applications may also be leveraged. If a third-party audit reporting application is used, implementation of the *P2Sentinel* Listener is highly recommended as best practice for interfacing data from the Millennium environment to the foreign application. Without it, there is potential for communication issues with residual impact on system performance in Millennium.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed via the AU/AR reports locally to end-user devices (e.g. temp files, cookies, caches).	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP).	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.

	Relied upon software: Cerner Millennium		
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification is available as of product version 2021. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification is available as of product version 2021. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(6) Transmission to Public Health Agencies — Antimicrobial Use and Resistance Reporting	Enables creation of antimicrobial usage and resistance reporting information formatted according to HL7 CDA standards for Healthcare Related Infection Reports. **Relied upon software**: Cerner Millennium	Required costs include software licenses for PowerChart, Pharmacy Inpatient, Medication Administration Record (MAR) or Point of Care, Cerner Microbiology or discrete Microbiology interface with susceptibility results and organisms, Discern Explorer, and AUR reporting extract subscription. Cerner MPages licensing with installation of version 5.2+ is optional for the associated Antimicrobial Stewardship Worklist.	Required costs accommodate the following pre-requisites for the certified capabilities: (1) MAR or Point of Care for recording medication administration data (2) Pharmacy Inpatient for order catalog linkage to MAR/Point of Care (3) Cerner Microbiology or discrete interface for structured microbiology and susceptibility results The certified reporting capabilities require up-front configuration to define antimicrobials and susceptibility results in Millennium Core Code Builder, and National Healthcare Safety Network (NHSN) location mapping. Operations processes must be implemented to support data loads for the reporting period, including historical data. Use of self-developed components/workflows beyond the scope of the standard reporting design assumptions may result in non-reportable data.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Electronic Case Reporting *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique user identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Access to the Health IT module is limited to Cerner associates for maintenance and troubleshooting activities. No PHI is available to users accessing the Health IT module. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of ePHI disclosure via electronic case reports, including integrity protection of recorded audit logs. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Reporting capabilities for audit events and data from the certified product require use of an external audit repository and reporting application to which audit data is securely transmitted after capture supporting physical separation of the audit log from the HIT module that is the subject of the audit in accordance with good security practices. During implementation, audit data is configured to be securely transmitted to either an instance of Cerner's certified *P2Sentinel* audit reporting application or a third-party audit reporting application. If a third-party audit reporting application is used, audit event data is transmitted outbound to the audit log repository in XML format according to the Audit Trail and Node Authentication (ATNA) profile standard message structure. Accordingly, the data may be subject to customization or modification to conform to the inbound formatting requirements of any such third-party application. Additionally, implementation of the *P2Sentinel* Listener is highly recommended as best practice for interfacing data from the certified product to the foreign application. Without it, there is potential for communication issues.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Use of *P2Sentinel* as the audit repository and reporting application is recommended and is subject to additional licensing costs. If a certified third-party audit reporting application (e.g. Fair Warning) is used in place of *P2Sentinel*, a license for the P2Sentinel Listener is recommended (but not required).	Reporting capabilities for audit events and data from the certified product require use of an external audit repository and reporting application to which audit data is securely transmitted after capture supporting physical separation of the audit log from the HIT module that is the subject of the audit in accordance with good security practices. During implementation, audit data is configured to be securely transmitted to either an instance of Cerner's certified *P2Sentinel* audit reporting application or a third-party audit reporting application. If a third-party audit reporting application is used, audit event data is transmitted outbound to the audit log repository in XML format according to the Audit Trail and Node Authentication (ATNA) profile standard message structure. Accordingly, the data may be subject to customization or modification to conform to the inbound formatting requirements of any such third-party application. Additionally, implementation of the *P2Sentinel* Listener is highly recommended as best practice for interfacing data from the certified product to the foreign application. Without it, there is potential for communication issues.

§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed via the AU/AR reports locally to end-user devices (e.g. temp files, cookies, caches). **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification is available as of product version 1. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification is available as of product version 1. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(5) Transmission to Public Health Agencies — Electronic Case Reporting	Enables automated creation of electronic case reports for public health reporting based on reportable condition triggers. **Relied upon software**: eCR Now FHIR App, Cerner Millennium	Required costs include a software license and one-time set up fee for Electronic Case Reporting, along with pre-requisite software licenses for PowerChart, Cerner Direct Messaging, Cerner Controlled Medical Terminology (CMT) content subscription for SNOMED-CT, ICD-10, and LOINC standard vocabulary code sets, and an annual subscription and one-time set up fee for Ignite Millennium API.	To enable the certified capability to be used, a data rights agreement must be completed for participation in the American Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform leveraged for processing case reporting via the eCR Now FHIR App. Additionally, a 4-6 week implementation and onboarding process must be completed, including cloud ontology mappings for aligning case report data with standard terminologies. Maintaining currency with standard content releases for SNOMED-CT, ICD-10, and LOINC is highly recommended. Currently, the Electronic Case Reporting certified capabilities support COVID-19 condition reporting exclusively. Achieving active engagement with a state department of public health for eCase Reporting using the certified product may require additional dedicated onboarding and testing activities for state-specific requirements and/or specifications.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Health Data Intelligence: eCQMs

See Appendix A for certified versions and CHPL listing information. See Appendix B for comprehensive list of certified Clinical Quality Measures.

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed for use of the EHI Export capabilities.	The HDI EHI Exports are requested through the Longitudinal Record Bulk Extract API. The extract is made available for download through the Data Syndication API. Once requested, the download is available for 21 days. To send requests to the APIs, you need an Oracle system account that includes a bearer token, and a set of OAuth credentials called the consumer key and consumer secret. For detailed steps to take to get system access see Getting-started. Before requesting an EHI Export, Oracle Health must enable the Longitudinal Record Bulk Extract API for your tenant and for the Data Syndication API, you must have at least one feed and at least one channel for that feed. Customers should contact their Health Data Intelligence engagement leader or log a service record (SR) in eService to the to request the enablement of Longitudinal Record Bulk Extract API and a new feed for the Longitudinal Record Bulk Extract feed type. More information and guidance on using the HDI EHI Export – including data format specifications for the outputs – are available with the public EHI Export documentation at https://www.oracle.com/health/regulatory/certified-health-it/#ehi-export-lnk (see the "Health Data Intelligence (HDI)" sub-heading).
§ 170.315(c)(1) CQMs – Record & Export	Includes the capability to record the data required for Clinical Quality Measure (CQM) calculations in a codified manner appropriate for the measures to which the product is certified, and the ability for an authorized user to generate QRDA Category I and QRDA Category III data files for export. **Relied upon software**: N/A	Required costs include a subscription to one of the following: Oracle Health Analytics Intelligence, Oracle Health Clinical Intelligence, or Oracle Health Care Coordination Intelligence*. Additional data source onboarding costs may apply, depending on data source type. *Legacy product ownership may also provide access to the certified capabilities.	Health Data Intelligence is an EHR-agnostic cloud-based population health management system. On-demand QRDA file generation and export are not typically intended for interactive data review/management purposes as reports are available within the system for such purposes. Pre-requisites for generation and export of QRDA data files include the following implementation and configuration tasks: establishing a Health Data Intelligence tenant (*one-time*), onboarding necessary clinical and encounter data (*variable based on source type*), deploying the Oracle Health Data Submissions application (*one-time*) and provisioning access for authorized users (*continual as needed*); deploying eCQM content (*annual request with automated releases thereafter*); and eCQM setup and validation (*annual).* Generation and export of QRDA data files is available on-demand in the Oracle Health Data Submissions application for appropriately licensed clients where all pre-requisite implementation and configuration tasks have been completed. Only patients who meet the initial patient population of an eCQM will qualify for QRDA file generation and only elements associated to the eCQMs selected for QRDA generation will be included. By default, eCQMs will be configured to refresh on a weekly cadence. Limited eCQM data refreshes can also be performed on an ad hoc basis, which requires a request to be submitted to Oracle. An eCQM refresh will apply to both measure outcome reports and QRDA file generation and can take 24-36 hours depending on tenant size. On-demand QRDA data file generation is available for the current and immediate previous measure specification version, for the measurement period(s) that have been deployed as requested. Measure deployment and subsequent file generation is supported

			for dates that fall within the current or previous calendar year to which the measure specifications and QRDA file specifications apply. For example, date ranges within CY 2024 are available for generation using the applicable measure and QRDA file specifications for program year (PY) 2024 or PY 2025. Export of QRDA data files where the date range differs from the measure and QRDA file specification by more than one year are considered beyond scope of the certified capabilities.
§ 170.315(c)(2) CQMs – Import & Calculate	Includes the capability for an authorized user to import QRDA Category I data files and perform Clinical Quality Measure (CQM) calculations for the data for the measures to which the product is certified. **Relied upon software**: N/A	Required costs include a subscription to one of the following: Oracle Health Analytics Intelligence, Oracle Health Clinical Intelligence, or Oracle Health Care Coordination Intelligence*. Additional data source onboarding costs may apply, depending on data source type. *Legacy product ownership may also provide access to the certified capabilities.	QRDA data file import can be used to supplement or replace EHR or claim source onboarding for the purposes of executing eCQMs. Patients and data included in QRDA import will create or add to an existing patient longitudinal record. Pre-requisites for import of QRDA data files include the following implementation and configuration tasks: establishing a Health Data Intelligence tenant (*one-time*), submitting a request for Oracle to create a structural mapping for QRDA (*once per QRDA source and QRDA version*) and configuring a QRDA data file upload process (*one-time*). Once the prerequisite setup is complete, QRDA import can be performed without subsequent developer assistance. The capability to import QRDA data files from an external third-party source system is available for appropriately licensed clients with pre-requisite configuration and implementation tasks completed. Imports are processed via standard Health Data Intelligence data ingestion processes and require the appropriate user authorization and authentication to submit QRDA data files for ingestion. Once QRDA data file import is processed successfully, patient data is visible within the longitudinal record and all Health Data Intelligence products. Data availability in downstream products is subject to processing time. Additional setup is required to enable inclusion in on-demand QRDA data file generation and export, or with electronic report submission. QRDA data file import capabilities support annual specifications for the current year on a rolling basis and are specific to the CMS and HL7 specifications for the same reporting year. Import of QRDA data files is available for both patients with or without an existing person record. Imported QRDA data files will be assessed by Oracle's Master Person Management product for patient deduplication utilizing a sophisticated patient matching algorithm.
§ 170.315(c)(3) CQMs – Report	Includes the capability to create QRDA Category I and III data files for reporting submission for the measures to which the product is certified. **Relied upon software**: N/A	Required costs include a subscription to one of the following: Oracle Health Analytics Intelligence, Oracle Health Clinical Intelligence, or Oracle Health Care Coordination Intelligence*. Additional data source onboarding costs may apply, depending on data source type. *Legacy product ownership may also provide access to the certified capabilities.	Health Data Intelligence: eCQMs supports eSubmission for regulatory programs (e.g. CMS eCQMs). For those clients using Oracle as their data submission vendor, and who rely on services to support that eSubmission, specific timeline requirements apply for registration of intent to use Oracle as a data submissions vendor and for making data available from the source clinical system(s). Pre-requisite implementation and configuration tasks also apply and include the following: establishing a Health Data Intelligence tenant (*one-time*), onboarding necessary clinical and encounter data (*variable based on source type*), deploying the Oracle Health Data Submissions application (*one-time*) and provisioning access for authorized users (*continual as needed*); deploying eCQM content (*annual request with automated releases thereafter*); and eCQM setup and validation (*annual).* Generation of QRDA data files for eSubmission is available to clients within the Oracle Health Data Submission application. Generation of QRDA data files for purpose of making data available to a third-party vendor for eSubmission or ancillary purpose is not a use-case within scope of this criterion and is instead enabled via use of capabilities under 170.315(c)(1).
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e., username/password) to gain access to patient health information in Oracle Health Data Submissions and other Health Data Intelligence applications.	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	N/A

	Relied upon software: N/A		
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of access to and actions on ePHI within the Oracle Health Data Submissions application, including integrity protection of recorded audit logs. **Relied upon software**: N/A	No associated costs or fees – the security auditing capabilities provided by the cloud auditing service are considered embedded with the licensing of the Health IT module itself.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. The cloud auditing service is not able to be disabled once deployed and does not require or support management of specific events of interest to be logged as the big data foundation model follows an approach of always sending everything.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, date and time of event, etc. **Relied upon software**: N/A	No associated costs or fees – audit reporting capabilities are available through the Privacy Analytics certified audit reporting application or via export of audit data for import to a third-party audit reporting application for no additional fees.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. Successful use of exported audit data in third-party reporting applications may require additional customization or modification of the event formatting to align with inbound formatting requirements of the third-party.
§ 170.315(d)(5) Automatic Access Time-out	Enables automatic termination of a user session in the Oracle Health Data Submissions application after a specified period of inactivity, defined at tenant level for customer. **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	The automatic time-out capability is enabled by default and set to execute at a standard inactivity period for all clients/users. This time-out feature is leveraged across all Health Data Intelligence applications.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. **Relied upon software:** N/A	No associated costs or fees	Oracle Health Data Submissions leverages the Health Data Intelligence platform's SSO infrastructure, which is capable of encrypting authentication credentials, with, at minimum, algorithms detailed in FIPS 140-2.
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. **Relied upon software:** N/A	No associated costs or fees	N/A
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

HealtheAnalytics: Promoting Interoperability

See Appendix A *for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(g)(2) Automated Measure Calculation	Enables calculation of numerator and denominator values for the following Stage 3 Promoting Interoperability (PI) measures for performance/reporting year 2019+: Medicare PI • ePrescribing (EH/CAH & EC) • Verify Opioid Treatment Agreement (EH/CAH & EC) • Support Electronic Referral Loops by Sending Health Information (EH/CAH & EC) • Support Electronic Referral Loops by Receiving and Incorporating Health Information (EH/CAH & EC) • Provide Patients Electronic Access to Their Health Information (EH/CAH & EC) Medicaid PI (EP only) • *Clinical Information Reconciliation • *Computerized Physician Order Entry (CPOE) • ePrescribing • *Patient Education • *Patient Generated Health Data • Provide Patients Electronic Access to Their Health Information • *Receive and Incorporate • *Secure Messaging • Support Electronic Referral Loops by Sending Health Information • *View, Download, Transmit *Measures officially recognized as certified as of July 7, 2020 **Relied upon software**: N/A	Required costs include a subscription for HealtheAnalytics.	Standard functional reports for automated measure calculation are designed to work in coordination with Cerner certified module capabilities and workflows. Information on the design assumptions of the reports is available in Cerner Reference Pages documentation. Use of self-developed components or use of workflows that are beyond the scope of the design assumptions of the standard reporting may not result in measurement consideration. Use of self-developed reporting or process to compile numerator and denominator data from different sources than Cerner certified modules is outside the scope of the certified capabilities. A data agreement for cloud storage of reporting data must also be in place for use of the certified capabilities. To enable the certified capability to be used configuration in the Cerner *Bedrock* wizard for definition of denominator populations and for measure definitions is required. Operations processes must also be implemented to support data processing from the applicable *Cerner Millennium* environment to the *HealtheAnalytics* platform. This requires a one-time onboarding process that must be performed by Cerner at no additional cost to the client. Due to potentially large data volumes, timeout limitations may occasionally be encountered. In some instances where data volume is especially high, resolution could require separation of data into multiple files for processing. The current and one previous version of the following browsers are supported: *Apple Safari*, *Google Chrome*, *Microsoft Internet Explorer*, *Microsoft Edge*, *Mozilla Firefox*.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A

§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

HealthSentry *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to the *HealthSentry* application, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Configuration of user accounts with associated security privileges, authentication parameters, and related access controls is required for use of the certified capability. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Support event creation capabilities for security auditing of processing and disclosure of ePHI by the *HealthSentry* application, including integrity protection of recorded audit logs. Cures Update criterion certification available as of product version 2021. **Relied upon software**: ntpd (Linux)	No associated costs or fees – the security auditing capabilities provided by the cloud auditing service are considered embedded with the licensing of the Health IT module itself.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. The cloud auditing service is not able to be disabled once deployed and does not require or support management of specific events of interest to be logged as the big data foundation model follows an approach of always sending everything.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2021. **Relied upon software**: ntpd (Linux)	No associated costs or fees – audit reporting capabilities are available through the Privacy Analytics certified audit reporting application or via export of audit data for import to a third-party audit reporting application for no additional fees.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. Successful use of exported audit data in third-party reporting applications may require additional customization or modification of the event formatting to align with inbound formatting requirements of the third-party.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed via the *HealthSentry* application locally to end-user devices (e.g. temp files, cookies, caches). **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2021. **Relied upon software:** N/A	N/A	N/A

170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2021. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(2) Transmission to Public Health Agencies — Syndromic Surveillance	Enables creation and transmission of public health surveillance data to external public health agencies formatted according to the HL7 2.5.1 standards for Syndromic Surveillance. **Relied upon software**: N/A	Required costs include a data subscription for HealthSentry and professional data services. Optional costs include data services connections to additional public health agencies.	*HealthSentry* will continue to support both Modified Stage 2 and Stage 3 reporting for existing clients, but does not support requirements beyond the PHIN Messaging Guide for Syndromic Surveillance (Release 2.0) National standard dataset (such as optional data elements or submissions more frequently than once every 24 hours) and is no longer available for new footprint implementations. If you would like to pursue Syndromic Surveillance reporting and are not currently live on HealthSentry, the new architecture option under product name *Syndromic Surveillance* must be pursued. Successful implementation of the certified capability requires configuration of a data feed for data extraction from Cerner Millennium to *HealthSentry*, and completion of onboarding activities with local or state public health jurisdiction, including registration of intent. If a third-party registration system is in use, data must be discretely interfaced to Cerner Millennium for the subsequent data feed extraction to HealthSentry.
§ 170.315(f)(3) Transmission to Public Health Agencies — Reportable Laboratory Tests and Value/Results	Enables creation and transmission of laboratory tests and results data to external public health agencies formatted according to the HL7 2.5.1 standards for Electronic Laboratory Reporting to Public Health. **Relied upon software**: N/A	Required costs include a data subscription for HealthSentry and software licenses for General Laboratory and Microbiology, or third-party lab system. Professional data services costs are also required. Optional costs include data services connections to additional public health agencies.	*HealthSentry* will continue to support both Modified Stage 2 and Stage 3 reporting for existing clients, but does not support requirements beyond the *HL7 2.5.1 Electronic Laboratory Reporting to Public Health Implementation Guide (Release 1)* National standard dataset (such as optional data elements or submissions more frequently than once every 24 hours) and is no longer available for new footprint implementations. If you would like to pursue Electronic Laboratory Results reporting and are not currently live on HealthSentry, the new architecture option under product name *Electronic Lab Results* must be pursued. Successful implementation of the certified capability requires configuration of a data feed for data extraction from Cerner Millennium to *HealthSentry*, and completion of onboarding activities with local or state public health jurisdiction, including registration of intent. If a third-party LIS is used, data must be discretely interfaced to Cerner Millennium for the subsequent data feed extraction to *HealthSentry*.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Millennium (Clinical) *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(a)(1) Computerized Physician Order Entry (CPOE) – Medications	Includes the capability to electronically record, change, and access a patient's medication orders. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders, and a Multum content subscription. Ongoing support costs are required based on the solution licenses.	As part of the appropriate use of the certified capability, clients are expected to maintain currency with *Multum* content updates to have accurate reflection of the current RxNorm code set. Use of Cerner-provided ancillary departmental ordering conversations, such as are available within *PharmNet*, are not considered to be within scope of the certified capabilities. Availability of medication orders for CPOE requires configuration and ongoing maintenance of a pharmacy order catalog and appropriate role-based security.
§ 170.315(a)(2) Computerized Physician Order Entry (CPOE) – Laboratory	Includes the capability to electronically record, change, and access a patient's laboratory orders. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders. Ongoing support costs are required based on the solution licenses.	Use of Cerner-provided ancillary departmental ordering conversations, such as are available within *PathNet*, are not considered to be within scope of the certified capabilities. Availability of laboratory orders for CPOE requires configuration and ongoing maintenance of a laboratory order catalog and appropriate role-based security.
§ 170.315(a)(3) Computerized Physician Order Entry (CPOE) – Diagnostic Imaging	Includes the capability to electronically record, change, and access a patient's diagnostic imaging orders. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders. Ongoing support costs are required based on the solution licenses.	Use of Cerner-provided ancillary departmental ordering conversations, such as are available within *RadNet*, are not considered to be within scope of the certified capabilities. Availability of diagnostic imaging orders for CPOE requires configuration and ongoing maintenance of an imaging order catalog and appropriate role-based security.
§ 170.315(a)(4) Drug-drug, Drug-Allergy Interaction Checks for CPOE	Includes the capability to detect and alert end-users of drug-drug and drug-allergy interactions when placing medication orders, and the ability to manage the severity level by which interaction alerts are triggered. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders, and a Multum content subscription for mCDS.	As part of the appropriate use of the certified capability, clients are expected to maintain currency with *Multum* content updates to have accurate reflection of the current RxNorm code set and drug-drug/drug/allergy interaction content, including reference sources. Use of other *Multum* content is outside the scope of the certified capabilities. Successful implementation of the certified capabilities requires Multum content installation and enabling of preferences for drug-drug/drug-allergy interaction checking. Clients can configure preferences to fit their individual policies for alert levels (e.g. moderate, major, contraindicated, etc.). Drug-allergy interaction checking is not supported for inactive ingredients that may be included in medications (e.g., food-based ingredients) or IV solution base components (e.g., dextrose, sodium chloride, etc.). Full details are published in Cerner's *Managing Cerner Multum Content* Reference Page.
§ 170.315(a)(5) Demographics	Includes the capability to electronically record, change, and access certain patient demographics – including race & ethnicity, preferred language, birth sex, and sexual orientation & gender identity – in accordance with defined vocabulary standards & code sets. **Relied upon software**: N/A	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP). A software license for Cerner Practice Management or Cerner Registration Management are optional costs as clients can also choose to utilize Millennium Core Registration at no cost, or an inbound interface from a third-party registration system. The modernized Oracle Health Patient Administration Cloud Service may also be utilized for an additional subscription fee.	Demographics response values are not required to be natively captured in registration conversations within Millennium, but mapping to defined standards must be in place regardless of the upstream data source. Existing registration conversations may require updates to enable recording that a patient declines to specify for applicable demographic elements, and multi-select capability for race and ethnicity. Successful implementation of the certified capabilities requires mapping of local Millennium response values to the defined standards for each demographic category using code value aliasing. Where a third-party registration system is used with an inbound interface, this depends on accurate inbound aliasing of response values upstream when interfaced from the source system. The ability of the source system to support use of the required code sets or to enable multi-select capability for

			race and ethnicity should also be assessed for any downstream impacts on the certified capabilities within Millennium. For the modernized Oracle Health Patient Administration Cloud Service capabilities, onboarding to Oracle Cloud Infrastructure (OCI) will also be a prerequisite. The certified capabilities also provide flexibility for supporting recording of Sexual Orientation and Gender Identity (SO/GI) information using either the Millennium Social History module for a clinical workflow or capturing through registration conversations, or both. If both methods are utilized, the values are synchronized to ensure that capture in one location is correctly reflected in the other. Sexual Orientation and Gender Identity (SO/GI) recording requires separate mapping of local responses to defined standards via *Cerner Knowledge Index* concepts, and standard functionality does not support inbound interfacing of SO/GI data from a third-party source system.
§ 170.315(a)(12) Family Health History	Includes the capability to electronically record, change, and access a patient's family health history using SNOMED-CT vocabulary for documented conditions. **Relied upon software**: N/A	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and a Cerner Controlled Medical Terminology (CMT) content subscription for SNOMED-CT mapping.	The certified capabilities assume that recording is performed via the Millennium Histories control; use of non-certified or custom components is outside the scope of the product's certification and may limit availability of data for downstream functionality. Successful implementation of the certified capabilities may require mappings for the current form of capture of first-degree relations to the National Human Genome Research Institute code set values.
§ 170.315(a)(14) Implantable Device List	Includes the capability to manage a list of a patient's implantable devices, including recording and parsing Unique Device Identifiers (UDI) and to support automated retrieval of additional device attributes from the Global Unique Device Identifier Database (GUDID). **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP). Supply Chain Point of Use or Departmental Clinical Supply Chain for Surgery with Surgical Management and barcode scanner hardware are optional costs for automated recording/parsing of Unique Device Identifiers (UDI) via barcode scanning.	While utilization of barcode scanning to record and parse a UDI is not specified in the certification criterion, it is recommended for use to provide for an optimal end-user workflow. Successful implementation of the certified capabilities requires configuration of the Implant History control and enabling of the GUDID query service. If the recommended barcode scanning capability is implemented, successful automated recording and parsing of the UDI via scan is dependent upon item reference data being pre-built in the Cerner Item Master at the manufacturer catalog item level with associated UPN Device Identifier (DI) defined. If barcode scanning is <u>not</u> implemented, recording and parsing of UDIs will require manual entry in the Implant History record, including the DI for GUDID querying. Standardized interfacing of UDIs from a third-party system to the Cerner Implant History module, whether in parsed or un-parsed state, is not supported. If initial capture of UDIs for implantable devices occurs in a separate upstream software application, recording and parsing of the UDIs will require manual re-transcription into Cerner's Implant History control.
§ 170.315(b)(1) Transitions of Care	Includes the capability to create transition of care documents in accordance with the HL7 Consolidated Clinical Document Architecture (C-CDA) Release 2.1 standards inclusive of required data element categories, and to subsequently exchange them using secure Direct messaging standards. Also included is the capability to receive and display transition of care (ToC) C-CDA documents in human-readable format and to detect conformance errors. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP), Cerner Direct Messaging (*one-time set up fees also apply), and CAMM Digital Objects, a Cerner Controlled Medical Terminology (CMT) content subscription for SNOMED-CT, ICD-10, LOINC, HL7, CDC & OMB standard code sets for race & ethnicity, RFC5646 standard for preferred language, UCUM, CPT-4, and HCPCS, and a Multum content subscription for RxNorm, CVX, and NDC. Optional costs include Advanced Interoperable Solutions (AIS) license and associated set up fees for XDR/XDM, and an additional software license for Cerner Direct Web Inbox enabling exchange with a recipient community provider who does not otherwise have Direct messaging capabilities. If opting for set up of a custom Direct messaging domain for	Exchange using the product's certified capability is based on use of the ONC Applicability Statement for Secure Health Transport; use of any other secure electronic transport formats or protocols is not a valid use of the certified capabilities. Based on Promoting Interoperability program measure definitions, other electronic transport methods may be used and qualify for measurement, but such use-cases would fall outside the scope of the product's certified capabilities. If not utilizing *Cerner Direct Messaging* for secure clinical document, a license with a third party HISP would be required along with a Cerner license for AIS to enable XDR connectivity (*Cerner Direct Messaging licensing also still required). *Cerner Direct Messaging* messaging is isolated to verified exchange partners under the active DirectTrust Trust Bundles for bi-directional communication (send and receive), and National Association for Trusted Exchange ("NATE") for unidirectional communication (send only). Generally, exchange outside these trusted networks is not needed, but should a client determine additional exchange partners are necessary, a service request can be logged to Cerner indicating the third-party HISP with which communication is desired, along with a business contact from that third-party HISP to begin the process. Cerner will facilitate the initial and ongoing third-party

		the Cerner Direct Inbox (versus building as an extension of the primary Cerner Direct domain for the Millennium environment), an additional software license is required. An additional software license may be required to enable Direct exchange communication with recipients beyond those serviced by HISPs participating in the active DirectTrust Trust Bundles for bi-directional communication (send and receive), and National Association for Trusted Exchange ("NATE") for unidirectional communication (send only).	contract maintenance, technology development, testing, and support required to maintain these one-off connections. All third-party HISPs are required to sign Cerner's connection agreement providing basic protections to both Cerner and our clients. There is no cost to the third-party HISP to participate in this agreement. Clients choosing this additional connectivity inherit Direct communication capabilities with all approved third-party HISPs submitted by other clients participating in the same software license. Use of the certified capabilities requires Message Center, *Clinical Reporting XR*, and the Clinical Document Generator (CDG) service. Use of the Direct External Address Book, ToC Operations Job, *MPages*, *Resonance* (document exchange), and *CommonWell* are optional. Personnel who are involved in the use of the certified system for clinical document exchange should have a Direct Messaging address that is serviced by the *Cerner Direct Messaging*. Users must also ensure medical code sets for problems, medications, and medication allergies have been implemented to support codification for associated objective measurement requirements. Data conversion and mapping may be required for use of non-standard code sets. Use of non-standard data capture for problems, medications, and medication allergies is problematic for inclusion of those clinical data elements in meeting requirements for associated objective measure credit. For the Implantable Device List included in the Medical Equipment section of C-CDA documents, device entries with a UDI and a status of active (i.e. currently implanted) are included in the C-CDA. An additional enhancement to populate active Implant History entries *without* a UDI is also available for all certified code levels. The certified product receives and validates C-CDA documents formatted to both Release 1.1 and 2.1; use of any other C-CDA release would be outside scope of the certified capabilities. For C-CDA creation, the scope of this criterion is limited to the C-CDA Continuity of Care Document (CCD), Referral Note, and (for the inpatient setting only) Discharge Summary document templates. Use of any non-certified capability for the recording of required structured clinical data to be included in ToC documents may not be compatible with the certified capabilities for ToC creation.
§ 170.315(b)(2) Clinical Information Reconciliation and Incorporation	Includes the capability to accurately match a received transition of care C-CDA document to a local patient record and to reconcile problems, medications, and medication allergies data to produce a single consolidated reconciled list in the patient's Electronic Health Record (EHR) that can be included in subsequently generated transition of care C-CDA documents. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and Cerner *MPages*, and content subscriptions for Multum and Cerner Controlled Medical Terminology (CMT). For organizations who elect to voluntarily adopt enhanced clinical reconciliation capabilities via Cerner's Seamless Exchange offering, an additional monthly subscription and associated set up fees apply. Other pre-requisite costs for Seamless Exchange capabilities include a *software license for CAMM Digital Objects, and an **annual subscription and one-time set up fee for Cerner's Ignite Millennium API (for clients that host their own infrastructure (CHO), an additional one-time setup cost for additional infrastructure is required, and supplemental costs for RedHat Licenses, VMWare licenses, and ESX Host hardware may apply). *The CAMM Digital Objects cost is the same as that required for the 170.315(b)(1) criterion certification under the same Certified Health IT Module (no additional fees apply if CAMM is already licensed and implemented for that criterion).	For reconciliation capabilities to perform optimally it is vital that clients stay current on nomenclature content updates for allergies (*Multum*), problems (ICD-10, SNOMED CT), and medications (*Multum*). Successful implementation of the certified capabilities requires installation of *MPages* version 6.3 or higher with the Histories (problems), Home Medications, and Allergies Workflow components enabled and configured to allow for reconciliation of external/unverified data. For organizations who elect to voluntarily adopt enhanced clinical reconciliation capabilities via Cerner's Seamless Exchange offering, additional pre-requisites include the following: Millennium 2018.03 code base or higher, MPages version 6.16 or higher, cloud onboarding with HealtheIntent data onboarding, and Ignite API implementation with Fast Healthcare Interoperability Resources (FHIR) R4 mappings.

		**The Millennium Ignite API (the API) costs are the same as those required for the 170.315(g)(7)-(9) criteria certification under the same Certified Health IT Module (no additional fees apply if the API is already implemented for those criteria).	
§ 170.315(b)(3) Electronic Prescribing	Includes the capability to transmit and receive prescription messages according to National Council for Prescription Drug Programs' (NCPDP) 2017071 standard for the New, Change, Cancel, Refill, Fill Status, and Medication History transactions, along with enforcing leading/trailing zeros logic and mL dosing units for oral liquid medications. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP), PowerOrders, Cerner ePrescribe, and a Multum content subscription. For client-hosted (CHO) clients, additional costs for a VPN solution to securely connect the Millennium domain to Cerner's ePrescribing Hub may apply. Additionally, although out of scope for the criterion, ePrescribing of Controlled Substances (EPCS) may require additional licensing and costs if a client chooses to leverage that capability.	To transact on the Surescripts electronic prescribing network, prescribers must be registered with Surescripts and obtain an SPI (Surescripts Provider ID). With standard implementation, external Rx history data is available for outpatient encounters and at discharge only for inpatient and emergency department encounters. Availability of external Rx history data at admission for inpatient and emergency department encounters is subject to additional costs. The certified capability includes notification alert messages to providers for electronic prescription failures. If the transmission of a prescription order to a pharmacy fails for any reason, a routing error message will be sent to either the ordering provider's Message Center or their designate (pool). In addition to Surescripts pre-requisites, successful implementation and use of the certified capabilities requires that a provider's demographic information (address, phone, fax, identifiers) be configured in the Millennium environment. Millennium pharmacy order catalog (including Multum content updates) must also be maintained to reflect the commercial availability of prescription products.
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for encrypted device and/or cloud storage of the exported data.	Implementation and use of the single patient EHI Export capability involves several pre-requisites including a minimum *Cerner Millennium* code level, Oracle 19c+ database version, a minimum of 50 GB temporary storage available on application servers, and an SFTP storage location at ftp3.cerner.com for temporary storage of the export prior to being delivered to the requestor. Single patient EHI Export also includes an optional data filtering feature intended for configuring exclusion of data from the export at the client's discretion. This feature is intended for exclusion of non-EHI data and organizations should take care to ensure that its use does not create potential violations of relevant regulations, including HIPAA Privacy and Information Blocking. Due to the data volume and overall complexity of the operations, patient population EHI Export is executed via engagement with Cerner resources. Clients can initiate an export by logging a request as directed on the *Understand Patient Population EHI Export* reference page. Please note that filtering the export by specific locations or other subsets within a *Cerner Millennium* system is not supported, nor is combining EHI across disparate *Cerner Millennium* systems. The following will be required for executing and taking possession of a patient population export: • An encrypted device provided by the customer to load the export on • Local hardware and storage of appropriate size for the export with Oracle licensed software to restore the export after receipt • Oracle Health Multimedia Storage 7 for the multimedia content export – customers whose data is stored on predecessor versions of Oracle Health Multimedia Storage will need to have content transitioned as part of the export process, which will impact delivery timelines. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).

§ 170.315(b)(11) Decision Support Interventions	Supports ability to select evidence-based and predictive decision support interventions (DSI) to deploy as part of the EHR system, along with end-user access to extensive reference information (source attributes) about DSIs supplied as part of the certified EHR and to record and export real-time electronic feedback about DSIs they're presented with in workflow. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP), and the Oracle Health FHIR APIs to support integration of third-party predictive DSIs in the form of SMART apps.	Access to source attribute information for Cerner-supplied DSIs and ability to record/modify DSI source attributes is available through the centralized DSI Reference Library component. Configuration is required to enable access to the certified capabilities and privileges must be granted to specific users that the organization desires to provide with ability to add and modify source attribute information. Some source attributes for Cerner-supplied DSIs are also made available through the Discern Development application, which requires installation of special packages to access the content. Configuration is also required to use the certified capabilities for recording and exporting real-time end-user feedback on DSIs. DSI feedback reports are accessible through standard Discern Analytics 2.0 reporting application framework which must also be installed in the environment as a pre-requisite. Ability to select third-party predictive DSIs for integration into the certified EHR is supported through use of publicly available FHIR APIs which support the full USCDI v3 value set. Accordingly, only predictive DSIs compatible with HIR API technology will be supported for selection. Customers can follow instructions documented on the *Overview of Facilitating Predictive DSI with FHIR* reference page.
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Configuration of Millennium Core Security for user account security privileges, authentication parameters, and related access controls is required for use of the certified capability. As a part of standard implementation, defining and administering users, security roles, authorization and authentication parameters, and the like is required. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities, but are not incompatible with their use.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of access to and actions on ePHI via the *PowerChart* application, including integrity protection of recorded audit logs. **Relied upon software**: ntpd (Linux)	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Optional costs include the Privacy Analytics Listener to enable audit events to be sent from the Millennium platform on which the certified product operates to an external third-party audit reporting application. Additional services-related costs may apply for configuration of outbound audit event data to meet the formatting constraints of any such third-party audit reporting application.	Configuration of the Millennium Core Audit Service, including enabling of desired audit events for logging and hash algorithm for tamper detection of captured audit data, must be completed for use of the certified capabilities. If a third-party audit reporting application is used, configuration of audit events to be securely transmitted from Millennium is required. Audit event data is captured and transmitted outbound to the audit log repository in XML format according to the Audit Trail and Node Authentication (ATNA) profile standard message structure and may be subject to customization or modification to conform to the inbound formatting requirements of any such third-party application.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. **Relied upon software**: ntpd (Linux)	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Use of Privacy Analytics as the audit repository and reporting application is recommended and is subject to additional licensing costs if utilized. If a certified third-party audit reporting application (e.g., Fair Warning) is used in place of Privacy Analytics, a license for the Privacy Analytics Listener is recommended (but not required).	Reporting capabilities for audit events and data from the certified product that are captured via Millennium Core Audit Service require use of an external audit repository and reporting application to which audit data is securely transmitted after capture supporting physical separation of the audit log from the HIT module that is the subject of the audit in accordance with good security practices. Privacy Analytics is recommended as the audit reporting application, but third-party applications may also be leveraged. If a third-party audit reporting application is used, implementation of the Privacy Analytics Listener is highly recommended as best practice for interfacing data from the Millennium environment to the foreign application. Without it, there is potential for communication issues with residual impact on system performance in Millennium.

§ 170.315(d)(4) Amendments	Enables recording of an amendment to a patient record based on a patient request, as well as the patient requests for amendment to their health record, including identification of whether the amendment was approved or denied. **Relied upon software**: N/A	No mandatory costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. To the extent there is desire to leverage existing documentation capabilities (e.g. PowerForms or Clinical Documentation templates) to support documenting amendment requests, costs apply for licensing those components for their broader purpose, but no distinct or additional costs apply for their use in support of this capability.	It is assumed that client definition and use of amendment capabilities should be flexible based on their form and manner of recording patient requested amendments. Amendments of ePHI maintained in non-certified systems is beyond the scope of Cerner's certified capability but Cerner recognizes they may be in use for maintenance of ePHI beyond the scope of records maintained by the certified system. Documentation templates can be defined both for recording patient requests/provider response and for the substance of the amendment request content. Accepting the amendment request into the record may involve use of additional documentation tools to create and maintain medical record entries out of amendment requests, such as for documenting a patient's home medications or recording patient contributed health information, depending on its form.
§ 170.315(d)(5) Automatic Access Time-out	Enables automatic termination of a user session after a specified period of inactivity requiring re-authentication. **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Use of the certified capability requires configuration at the Millennium application server level that is typically performed at a network administrator task for consistency across individual users and workstations.
§ 170.315(d)(6) Emergency Access	Enables a limited set of specified users to access electronic health information in emergency scenarios. **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Use of business continuity and disaster recovery techniques and tools are beyond the scope of the intent of emergency access capabilities within the certified product but are relevant for HIPAA Security compliance and overall security risk assessment processes. To enable the certified capability to be used, configuration of user positions with privilege to invoke the emergency access relationship type must be defined. This capability allows for override of restrictions on a user's ability to access records beyond the organization they are associated to, of encounter records marked as subject to confidentiality levels and based upon the access rights that may be defined for the emergency mode of access relationship type.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed in the *PowerChart* application locally to end-user devices (e.g. temp files, cookies, caches). **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
§ 170.315(d)(8) Integrity	Enables verification that health information exchanged electronically (both outbound and inbound) has not been altered during transmit via use of message digests produced by hash algorithms of SHA-2 or greater strength. **Relied upon software**: N/A	Required costs beyond the licensing required for the Health IT module include a software license for the Cerner Direct Messaging. ***NOTE** Cerner Direct Messaging is already a required license for the Health IT module by virtue of its support for the 170.315(h)(1) criterion	Integrity protection is enabled principally for secure transport of clinical information between entities for those end points and transacting capabilities intended for use with the certified Health IT module. Unsecure transport methods for transport of ePHI between entities may lead to risk of security vulnerability and are not recommended. Use of the certified capability requires full implementation and onboarding of the *Cerner Direct Messaging* for the given Millennium environment.
§ 170.315(d)(9) Trusted Connection	Enables the secure encryption and integrity-protection of electronic health information transmitted to external applications via API for patient access, and contribution of data to Millennium from external applications for patient health information capture. **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	For secure data exchange in the context of patient health information capture (170.315(e)(3)), full successful implementation is dependent upon Websphere application server (WAS) configuration including TLS v1.2 communications security and digital certificates with SHA-2 support. In the case of transmission to external applications via API for patient access (170.315(g)(7)-(9)), secure exchange is inherent with a full implementation of the Ignite Millennium API.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for	N/A	N/A

	market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2018. **Relied upon software:** N/A		
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
§ 170.315(e)(3) Patient Health Information Capture	Includes the capability for patients or their authorized representatives to securely and electronically provide health information from non-clinical settings to providers and care team members for incorporation into their health record. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and Advanced Care Documentation (PowerForms) for capture of hyperlinks to patient-provided health information in the EHR. The Messaging REST service through which data is transmitted inbound to Millennium is embedded with Cerner Millennium at no additional cost.	The product's certification for Patient Health Information Capture is compatible with the use of third-party patient portals or similar patient-facing applications as a data contribution source from which patients (or their authorized representatives) can securely and electronically share health information with their providers in Millennium. Due to the open nature of the Messaging REST service through which data is transmitted inbound to Millennium, no specific contract or agreement is required between Cerner and any third-party application developers to enable connection. Capture of patient-provided hyperlinks to patient health information is performed via use of a select PowerForm. Successful implementation of the certified capabilities requires up-front code installation and configuration of the Messaging REST service (RESTful API). For a third-party application (e.g. patient portal, mobile health app, etc) to be compatible as a data contribution source, it must be capable of calling an API over Hypertext Transfer Protocol Secure (HTTPS). Additional pre-requisite configurations requiring technical knowledge for the implementation also apply. Services are available for initial setup of the REST service to be called by a chosen third-party application, but further specifics are dependent on unique implementation considerations for the particular third-party application. Authentication and authorization from third-party applications accessing the REST service requires OAuth, for which configuration is an additional pre-requisite for client-hosted (CHO) clients. To positively identify and associate contributed data with a unique patient, a method for transmitting a patient identifier from Cerner to the third-party application to be passed back into Cerner with the data submissions is a pre-requisite for certified functionality. For credit on the associated objective measurement, patient-provided health information must be stored to the record by saving the message to chart. *_HealtheLife_ is also certified to the criterion and allows for a formal contribution method dependent on licensing and use of the HealtheLife patient portal's messaging feature.
§ 170.315(g)(2) Automated Measure Calculation	Enables calculation of numerator and denominator values for the following Stage 3 Promoting Interoperability (PI) measures for performance/reporting year 2019+: Medicare PI	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and Business Objects.	Standard functional reports for automated measure calculation are designed to work in coordination with certified product capabilities and workflows. Information on the design assumptions of the reports is available in Cerner Reference Pages documentation.

	• e-Prescribing (EH/CAH & EC) • *Verify Opioid Treatment Agreement (EH/CAH & EC) • *Support Electronic Referral Loops by Sending Health Information (EH/CAH & EC) • Support Electronic Referral Loops by Receiving and Incorporating Health Information (EH/CAH & EC) • Provide Patients Electronic Access to Their Health Information (EH/CAH & EC) *Measures officially recognized as certified for EH/CAH as of August 8, 2019 and for EC as of November 8, 2019 <u>Medicaid PI (EP only)</u> • Clinical Information Reconciliation • Computerized Physician Order Entry (CPOE) • ePrescribing • Patient Education • Patient Generated Health Data • Provide Patients Electronic Access to Their Health Information • Receive and Incorporate • Secure Messaging • Support Electronic Referral Loops by Sending Health Information • View, Download, Transmit **Relied upon software**: N/A		Use of self-developed components or use of workflows that are beyond the scope of the design assumptions of the standard reporting may not result in measurement consideration. Use of self-developed reporting or process to compile numerator and denominator data from different sources than the certified product is outside scope of Cerner's certified capabilities. To enable the certified capability to be used configuration in the Cerner Bedrock wizard for definition of denominator populations and for measure definitions is required. Operations processes must also be implemented to support data loads for the reporting period. If reporting requirements change because of CMS policy clarifications or due to identification of error correction needs in reporting logic, this can require historical loads of data to assure proper measure calculation and credit.
§ 170.315(g)(3) Safety Enhanced Design	Defines user-centered design processes and assessments for applicable certified capabilities within the certified product's scope. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(6) C-CDA Creation Performance	Enables the creation of a standards-conformant Consolidated Clinical Document Architecture (C-CDA) document, including Common Clinical Data Set (CCDS) representation.	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and CAMM Digital Objects, a Cerner Controlled Medical Terminology (CMT) content subscription for SNOMED-CT, ICD-10, LOINC, HL7, CDC & OMB standard code sets for race &	The C-CDA creation performance capabilities are supported as per ONC policy with certification of 170.315(b)(1), 170.315(b)(2), 170.315(b)(4), and 170.315(b)(6) criteria for creation of a C-CDA documents. Appropriate implementation and maintenance of medical code sets for vocabulary constraints and mapping of demographics data elements to defined standards is a pre-requisite for conformant C-CDA generation. Use of any non-certified capability for the recording of required

	Cures Update criterion certification available as of product version 2018 (requires a minimum sub-release of *Cerner Millennium* 2018.08). **Relied upon software**: N/A	ethnicity, RFC5646 standard for preferred language, UCUM, CPT-4, and HCPCS, and a Multum content subscription for RxNorm, CVX, and NDC.	structured clinical data to be included in C-CDA documents may not be compatible with certified capabilities. Use of the certified capabilities requires Message Center, Clinical Reporting XR, and the Clinical Document Generator (CDG) service. For the Implantable Device List included in the Medical Equipment section of C-CDA documents, device entries with a UDI and a status of active (i.e., currently implanted) are included in the C-CDA. An additional enhancement to populate active Implant History entries *without* a UDI is also available for all certified code levels. Criterion scope is limited to the CCD, Referral Note, and Discharge Summary C-CDA templates.
§ 170.315(g)(7) Application Access – Patient Selection	Includes the capability to uniquely match and authenticate a request for access to health information from an external application of the patient's choice via the *Cerner Ignite APIs for Millennium* to the correct Millennium patient record. **Relied upon software**: N/A	Required costs include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and an annual subscription and one-time set up fee for *Cerner Ignite APIs for Millennium* and *Cerner Ignite APIs for Millennium with bulk data access* (the API). Standard rates for the API products are published at https://www.cerner.com/certified-health-it under the Certified API Technology Fees heading. For clients that host their own infrastructure (CHO), an additional one-time setup cost for additional infrastructure is required, and supplemental costs for RedHat Licenses, VMWare licenses, and ESX Host hardware may apply. In most cases, initial implementation of the API within the client's environment will be covered under the client's setup license, but there may be cases of implementation complexity or volume where additional costs would be incurred. Potential interface services may be necessary at a cost to interface credentials and/or relationship information into Millennium for authorized representatives not otherwise known to the system until specified by the patient for ability to leverage the patient's consumer access. If a third-party Identity Provider (IdP) is being used for consumer access, a one-time cost will be associated with set up for either integrating the IdP with the API or for Cerner consumer IdP setup for the API. Developers or clients implementing direct to consumer applications (and therefore consumers themselves) will not be charged connection or usage-based fees.	To be considered "fully implemented" as required under EHR Incentive Program regulations, the API for API-based access and an Identity Provider (IdP) are required. Cerner provides a consumer IdP as the default IdP available for clients and/or their third-party patient access solutions to integrate with. Options for IdP include: (1) Cerner consumer IdP used for HealtheLife and the API, or (2) a third-party/client specified IdP able to be integrated with *HealtheLife* and the API, or (3) a third-party/client specified IdP used for consumer identity management plus Cerner consumer IdP separately for the API. Clients will be responsible ensuring patient identity proofing occurs before enabling access to health data electronically via the API, and that the identity proofing systems are integrated with the API. Clients will also be responsible for integrating applications with the API and ensuring patient identity proofing occurs when the third-party applications call the API. Connection of a third-party/client specified IdP with the API requires that the IdP support Security Assertion Markup Language (SAML) authentication standards for integration with the Cerner-hosted security services. Cerner maintains ontology mappings on clients' behalf and baseline mappings that expose a majority of clinical data in required terminologies are included by default with a standard implementation. However, through the course of application adoptions, content mapping gaps may be discovered. In such cases, clients will need to submit a request to Cerner to add additional mappings that a particular application being implemented may require. For the bulk data (multi-patient) API, active use requires an onboarding process for selected applications. This includes defining groups consisting of the specific patient identifiers for the group of patients matching the criteria of the use-case,. Additional details and guidance are available in Cerner's *Understand Cerner Ignite APIs for Millennium with Bulk Data Access* Reference Page.
§ 170.315(g)(9) Application Access – All Data Request	Includes the capability to respond to authenticated requests for health information via the *Cerner Ignite APIs for Millennium* with the full Common Clinical Data Set (CCDS) using the C-CDA Continuity of Care Document (CCD) template, including accommodation of specific dates/date ranges. **Relied upon software**: N/A		
§ 170.315(g)(10) Standardized API for Patient and Population Services	Includes the capability to respond to authenticated requests for health information via the *Cerner Ignite APIs for Millennium* for the full United States Core Data for Interoperability (USCDI) v1 data set. In accordance with applicable HL7® FHIR® and related privacy and security standards. This includes both Standalone (patient) and EHR (practitioner) launches for single patient context, as well as bulk data (multi-patient) retrieval for system personas. **Relied upon software**: N/A		
§ 170.315(h)(1) Direct Project	Includes the capability to exchange health information with external entities using the Direct Project standards for Secure Health Transport. **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP), Cerner Direct Messaging (*one-time set up fees also apply). Optional costs include licensing of Advanced Interoperable Solutions (AIS) for Edge Protocol (XDR/XDM).	Use of *Cerner Direct Messaging* requires that clients complete a current Cerner Direct Messaging certificate request containing required Trust Framework contents that establish and validate Clients' authenticity and parameters under which they may participate in Direct exchange. Use of the certified capability is limited to exchange with known, trusted users who have Direct accounts. Transacting with non-Direct users is outside the scope of the certified capability. Use of this capability by providers for transitions of care is optional as CMS permits other methods of electronic transacting for objective measurement. However, possession of the certified capability for this criterion is required as part of the CEHRT definition.

Millennium (CQMs) *See Appendix A for certified versions and CHPL listing information. See Appendix B for comprehensive list of certified Clinical Quality Measures.*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for encrypted device and/or cloud storage of the exported data.	Implementation and use of the single patient EHI Export capability involves several pre-requisites including a minimum *Cerner Millennium* code level, Oracle 19c+ database version, a minimum of 50 GB temporary storage available on application servers, and an SFTP storage location at ftp3.cerner.com for temporary storage of the export prior to being delivered to the requestor. Single patient EHI Export also includes an optional data filtering feature intended for configuring exclusion of data from the export at the client's discretion. This feature is intended for exclusion of non-EHI data and organizations should take care to ensure that its use does not create potential violations of relevant regulations, including HIPAA Privacy and Information Blocking. Due to the data volume and overall complexity of the operations, patient population EHI Export is executed via engagement with Cerner resources. Clients can initiate an export by logging a request as directed on the *Understand Patient Population EHI Export* reference page. Please note that filtering the export by specific locations or other subsets within a *Cerner Millennium* system is not supported, nor is combining EHI across disparate *Cerner Millennium* systems. The following will be required for executing and taking possession of a patient population export: • An encrypted device provided by the customer to load the export on • Local hardware and storage of appropriate size for the export with Oracle licensed software to restore the export after receipt • Oracle Health Multimedia Storage 7 for the multimedia content export – customers whose data is stored on predecessor versions of Oracle Health Multimedia Storage will need to have content transitioned as part of the export process, which will impact delivery timelines. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(c)(1) CQMs – Record & Export	Includes the capability to record the data required for Clinical Quality Measure (CQM) calculations in a codified manner appropriate for the measures to which the product is certified, and the ability for an authorized user to generate QRDA Category I and QRDA Category III data files for export. **Relied upon software**: Cerner Quality Reporting	Required costs include a Quality Reporting content subscription and software licenses for the following: PowerChart OR Emergency Medicine (FirstNet); SAP Business Objects for Lighthouse (or *HealtheEDW* or *PowerInsight* EDW or *PowerInsight* Explorer); PowerOrders; Advanced Care Documentation (PowerForms); Cerner HIM (or Abstracted Data Incoming)	The *Quality Clearinghouse* (QCH) is a centrally maintained clearinghouse that is embedded with the subscription to Cerner Quality Reporting – it is solely compatible with the electronic health record maintained in Cerner Millennium as a source clinical system and is not intended for use as a separate data warehouse. Use of on-demand generation and export of QRDA data files is intended for distinct use-cases, such as making data available to a third-party eSubmission vendor or registry capable of receiving QRDA data files and is distinct from electronic report submission capabilities and use-cases under 170.315(c)(3). On-demand generation and export is also not typically intended for interactive data review/management purposes as real-time dashboard views are available within the system for such purposes. Pre-requisites for generation and export of QRDA data files include the following implementation and configuration tasks: establishing a QCH connection for your Millennium environment and provisioning access for authorized users (*one-time*); package installation for eCQM and QRDA specification updates from CMS (*annual + monthly releases*); eCQM set up and validation (annual); eCQM data extraction/transfer from Millennium to the QCH (*one-time or variable depending upon needs*).

			Generation and export of QRDA data files is available on-demand in the QCH for appropriately licensed clients where all pre-requisite implementation and configuration tasks have been completed. Only eCQM data that has been extracted from the connected Millennium environment and transferred to the QCH will qualify for QRDA data file generation. Recommended set up includes configuration of an automated daily refresh of eCQM data available in the QCH (processing time for these daily extractions varies, but will typically complete within 2-3 days). eCQM data refreshes can also be performed on an ad hoc basis if preferred, but would require an extra step to initiate the extraction/transfer process manually for each refresh. On-demand QRDA data files are available for the current and immediate previous calendar year on a rolling basis. File generation is supported for dates that fall within the calendar year to which the measure specifications and QRDA file specifications apply. For example, date ranges within CY 2019 are available for generation using the applicable measure and QRDA file specifications for CY 2019. Export of QRDA data files where the date range differs from the measure and QRDA file specification year are considered beyond scope of the certified capabilities and require additional developer assistance. Detailed specifications for eCQM data loads is published in Cerner's *Overview of 2015 Edition Certification Criteria for Clinical Quality Measures* Reference Page. *For clients under Cerner's hosted/ASP models, pre-requisite tasks are typically performed by Cerner acting in the role of a user on behalf of the client as a part of the services agreement. Under these models, a service request must be logged for data extraction/transfer in all instances of QRDA export, whether as part of a recurring schedule of exports or ad hoc. *Detailed guidance for pre-requisite implementation and configuration tasks is published in Cerner's *Overview of 2015 Edition Certification Criteria for Clinical Quality Measures* Reference Page.
§ 170.315(c)(2) CQMs – Import & Calculate	Includes the capability for an authorized user to import QRDA Category I data files and perform Clinical Quality Measure (CQM) calculations for the data for the measures to which the product is certified. **Relied upon software**: Cerner Quality Reporting	Required costs include a Quality Reporting content subscription and software licenses for the following: PowerCHart OR Emergency Medicine (FirstNet); SAP Business Objects for Lighthouse (or *HealtheEDW* or *PowerInsight* EDW or *PowerInsight* Explorer); PowerOrders; Advanced Care Documentation (PowerForms); Cerner HIM (or Abstracted Data Incoming)	QRDA data file import is intended most typically for the integration of data from third-party clinical source systems for Quality Reporting purposes particularly to support consolidation of quality measurement data when clients transition from a third party EHR to Cerner mid-reporting period for one reporting submission. Import functionality does not create new medical record entries in the electronic health record maintained in Millennium and is not intended to be used as an alternative for foreign systems interfacing of source medical record data into the EHR as would be performed for medical record conversion across EHR systems. Pre-requisites for import of QRDA data files include the following implementation and configuration tasks: establishing a QCH connection for your Millennium environment and provisioning access for authorized users (*one-time*); eCQM and QRDA import package installation for CMS specification updates (*annual + monthly releases*); eCQM set up and validation (*annual*); setup of QRDA Shell Script and execution authorization for appropriate users (*one-time*). The capability to import QRDA data files from an external third-party source system is available for appropriately licensed clients with pre-requisite configuration and implementation tasks completed. Imports are processed via script execution in the Cerner Millennium domain to load the data and require appropriate user authorization and authentication to perform. Once QRDA data file import is processed successfully, additional steps are required for extraction of data to the QCH to enable inclusion in on-demand QRDA data file generation and export, or with electronic report submission. QRDA data file import capabilities support annual specifications for the current and

			immediate prior year on a rolling basis and are specific to the CMS and HL7 specifications for the same reporting year. Import of QRDA data files is available only for patients with an existing person record within the Cerner Millennium domain to which the file is being imported. QRDA data file and existing Millennium person ID are matched through an alias on the file that exists on the person record, or through a manual process of defining each link between QRDA data file and Millennium person record. Imported eCQM data is stored to the Quality Reporting schema in the Millennium environment, which is separate from the Millennium environment's clinical EHR database. Accordingly, while de-duplication of data for matching person identifiers is enabled across individual imported QRDA data files, de-duplication is not performed against the local Millennium EHR's patient records. De-duplication against local Millennium records would require interfacing of source clinical data to the Millennium clinical EHR database directly, which is out of scope for this criterion. *For clients under Cerner's hosted/ASP models, QRDA import is performed by Cerner acting in the role of a user as part of the clients' services agreement *For clients under Cerner's hosted/ASP models, pre-requisite tasks are typically performed by Cerner acting in the role of a user on behalf of the client as a part of the services agreement *Detailed guidance for pre-requisite implementation and configuration tasks is published in Cerner's *Overview of 2015 Edition Certification Criteria for Clinical Quality Measures* Reference Page.
§ 170.315(c)(3) CQMs – Report	Includes the capability to create QRDA Category I and III data files for reporting submission for the measures to which the product is certified. Cures Update criterion certification available as of product version 2018. **Relied upon software**: Cerner Quality Reporting	Required costs include a Quality Reporting content subscription and software licenses for the following: PowerChart OR Emergency Medicine (FirstNet); SAP Business Objects for Lighthouse (or *HealtheEDW* or *PowerInsight* EDW or *PowerInsight* Explorer); PowerOrders; Advanced Care Documentation (PowerForms); Cerner HIM (or Abstracted Data Incoming)	*FirstNet (CQMs)* supports eSubmission for regulatory programs (e.g. CMS or TJC eCQMs). For those clients using Cerner as their data submission vendor, and who rely on services to support that eSubmission, specific timeline requirements apply for registration of intent to use Cerner as a data submissions vendor and for making data available from the source clinical system(s). These are published on Cerner's *Eligible Provider Quality Reporting Reference Page* for Ambulatory clients, and on Cerner's *Meaningful Use Hospital eCQM Reference Page* for Hospital clients. Pre-requisite implementation and configuration tasks also apply and include the following: establishing a QCH connection for your Millennium environment and provisioning access for authorized users (*one-time*); package installation for eCQM and QRDA specification updates from CMS (*annual + monthly releases*); eCQM set up and validation (annual); eCQM data extraction/transfer from Millennium to the QCH (*one-time per submission*) Generation of QRDA data files for eSubmission is performed by Cerner on behalf of all clients who have registered intent to use Cerner as their data submission vendor. Generation of QRDA data files for purpose of making data available to a third-party vendor for eSubmission or ancillary purpose is not a use-case within scope of this criterion and is instead enabled via use of capabilities under 170.315(c)(1). eSubmission of QRDA data files is available for appropriately licensed clients with registered intent and requires extraction/transfer of data from the source Millennium environment to the QCH (pre-requisite connection of the source Millennium environment to the QCH must be in place). QRDA data files are generated from the QCH by Cerner for eSubmission and data qualification is constrained to the data loaded in Millennium for the chosen measures and associated reporting period.
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to electronic	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing	N/A

	health information in *FirstNet* and the *Quality Clearinghouse*, and includes the ability to control the specific access and privileges a user is granted. **Relied upon software**: N/A	is required for the certified capability apart from the licensing required for the Health IT module.	
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of access to and actions on ePHI within the *Quality Clearinghouse*, including integrity protection of recorded audit logs. Cures Update criterion certification available as of product version 2018. **Relied upon software**: ntpd (Linux)	No associated costs or fees – the security auditing capabilities provided by the cloud auditing service are considered embedded with the licensing of the Health IT module itself.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. The cloud auditing service is not able to be disabled once deployed and does not require or support management of specific events of interest to be logged as the big data foundation model follows an approach of always sending everything.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2018. **Relied upon software**: ntpd (Linux)	No associated costs or fees – audit reporting capabilities are available through the Privacy Analytics certified audit reporting application or via export of audit data for import to a third-party audit reporting application for no additional fees.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. Successful use of exported audit data in third-party reporting applications may require additional customization or modification of the event formatting to align with inbound formatting requirements of the third-party.
§ 170.315(d)(5) Automatic Access Time-out	Enables automatic termination of a user session in the *Quality Clearinghouse* after a specified period of inactivity **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	The automatic time-out capability is enabled by default and set to execute at a standard inactivity period for all clients/users.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the certified capabilities are developed, tested, implemented, and maintained.	No associated costs or fees	N/A

	Relied upon software: N/A		
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Millennium (Health Care Surveys) *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for encrypted device and/or cloud storage of the exported data.	Implementation and use of the single patient EHI Export capability involves several pre-requisites including a minimum *Cerner Millennium* code level, Oracle 19c+ database version, a minimum of 50 GB temporary storage available on application servers, and an SFTP storage location at ftp3.cerner.com for temporary storage of the export prior to being delivered to the requestor. Single patient EHI Export also includes an optional data filtering feature intended for configuring exclusion of data from the export at the client's discretion. This feature is intended for exclusion of non-EHI data and organizations should take care to ensure that its use does not create potential violations of relevant regulations, including HIPAA Privacy and Information Blocking. Due to the data volume and overall complexity of the operations, patient population EHI Export is executed via engagement with Cerner resources. Clients can initiate an export by logging a request as directed on the *Understand Patient Population EHI Export* reference page. Please note that filtering the export by specific locations or other subsets within a *Cerner Millennium* system is not supported, nor is combining EHI across disparate *Cerner Millennium* systems. The following will be required for executing and taking possession of a patient population export: • An encrypted device provided by the customer to load the export on • Local hardware and storage of appropriate size for the export with Oracle licensed software to restore the export after receipt • Oracle Health Multimedia Storage 7 for the multimedia content export – customers whose data is stored on predecessor versions of Oracle Health Multimedia Storage will need to have content transitioned as part of the export process, which will impact delivery timelines. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Configuration of user accounts with associated security privileges, authentication parameters, and related access controls is required for use of the certified capability. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of processing and disclosure of ePHI by the *PowerChart* application for generating and submission of National Health Care Surveys (NHCS) reports, including integrity protection of recorded audit logs. Cures Update criterion certification available as of product version 2018.	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Optional costs include the Privacy Analytics Listener to enable audit events to be sent from the Millennium platform on which the certified product operates to an external third-party audit reporting application. Additional services-related costs may apply for configuration of outbound audit event	Configuration of the Millennium Core Audit Service, including enabling of desired audit events for logging and hash algorithm for tamper detection of captured audit data, must be completed for use of the certified capabilities. If a third-party audit reporting application is used, configuration of audit events to be securely transmitted from Millennium is required. Audit event data is captured and transmitted outbound to the audit log repository in XML format according to the Audit Trail and Node Authentication (ATNA) profile standard message structure and may be subject to customization or modification to conform to the inbound formatting requirements of any such third-party application.

	Relied upon software: N/A	data to meet the formatting constraints of any such third-party audit reporting application.	
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2018. **Relied upon software**: N/A	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Use of Privacy Analytics as the audit repository and reporting application is recommended and is subject to additional licensing costs if utilized. If a certified third-party audit reporting application (e.g., Fair Warning) is used in place of Privacy Analytics, a license for the Privacy Analytics Listener is recommended (but not required).	Reporting capabilities for audit events and data from the certified product that are captured via Millennium Core Audit Service require use of an external audit repository and reporting application to which audit data is securely transmitted after capture supporting physical separation of the audit log from the HIT module that is the subject of the audit in accordance with good security practices. Privacy Analytics is recommended as the audit reporting application, but third-party applications may also be leveraged. If a third-party audit reporting application is used, implementation of the Privacy Analytics Listener is highly recommended as best practice for interfacing data from the Millennium environment to the foreign application. Without it, there is potential for communication issues with residual impact on system performance in Millennium.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed via the *PowerChart* application locally to end-user devices (e.g. temp files, cookies, caches). **Relied upon software**: N/A	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(7) Transmission to Public Health Agencies — Health Care Surveys	Enables creation of health care survey information formatted according to the HL7 Clinical Document Architecture (CDA) standards for National Health Care Surveys (NHCS) – specifically, version 1.2 of the Implementation Guide (IG). **Relied upon software**: N/A	Required costs include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP), and CAMM Digital Objects, and a Cerner Controlled Medical Terminology (CMT) content subscription for vocabulary standards mapping. A one-time fee for implementation services is recommended to ensure proper configuration of templates and data sources, but not required. Emergency Medicine (FirstNet) software license is also a recommended cost; if Cerner's FirstNet system is not used in the Emergency Department (ED), additional costs may be incurred for inbound	The certified capabilities are exclusively intended for purpose of submission to the Center for Disease Control's (CDC) National Center for Health Statistics (NCHS) NHCS registry. Any use for ancillary purpose would be outside the scope of the certified criterion. Participation in the NHCS registry is subject to CDC selection and request for active submission. The scope of this certification is also isolated to the creation of conformant NHCS Clinical Document Architecture (CDA) documents and does not include actual transmission of the data for submission to the registry. To enable the certified capability to be used, accurate population of required elements in the NHCS CDA templates is dependent on the activity and reference data being available in the appropriate location and format in the Cerner Millennium database. This may require adoption of new or

		interfacing of data required for ED encounters from third-party system to support applicable NHCS reporting submissions.	modified end-user workflows. For Emergency Department (ED) encounters required to be submitted for specific Survey classifications, this may require additional inbound interfacing of clinical event data if Cerner's FirstNet ED system is not in use.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Millennium (Immunizations) *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for encrypted device and/or cloud storage of the exported data.	Implementation and use of the single patient EHI Export capability involves several pre-requisites including a minimum *Cerner Millennium* code level, Oracle 19c+ database version, a minimum of 50 GB temporary storage available on application servers, and an SFTP storage location at ftp3.cerner.com for temporary storage of the export prior to being delivered to the requestor. Single patient EHI Export also includes an optional data filtering feature intended for configuring exclusion of data from the export at the client's discretion. This feature is intended for exclusion of non-EHI data and organizations should take care to ensure that its use does not create potential violations of relevant regulations, including HIPAA Privacy and Information Blocking. Due to the data volume and overall complexity of the operations, patient population EHI Export is executed via engagement with Cerner resources. Clients can initiate an export by logging a request as directed on the *Understand Patient Population EHI Export* reference page. Please note that filtering the export by specific locations or other subsets within a *Cerner Millennium* system is not supported, nor is combining EHI across disparate *Cerner Millennium* systems. The following will be required for executing and taking possession of a patient population export: • An encrypted device provided by the customer to load the export on • Local hardware and storage of appropriate size for the export with Oracle licensed software to restore the export after receipt • Oracle Health Multimedia Storage 7 for the multimedia content export – customers whose data is stored on predecessor versions of Oracle Health Multimedia Storage will need to have content transitioned as part of the export process, which will impact delivery timelines. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Configuration of Millennium Core Security for user account security privileges, authentication parameters, and related access controls is required for use of the certified capability. As a part of standard implementation, defining and administering users, security roles, authorization and authentication parameters, and the like is required. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities, but are not incompatible with their use.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of access to and actions on ePHI within *FirstNet* for activities related to immunizations reporting, including integrity protection of recorded audit logs.	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Configuration of the Millennium Core Audit Service, including enabling of desired audit events for logging and hash algorithm for tamper detection of captured audit data, must be completed for use of the certified capabilities.

	Cures Update criterion certification available as of product version 2018. **Relied upon software**: ntpd (Linux)	Optional costs include the Privacy Analytics Listener to enable audit events to be sent from the Millennium platform on which the certified product operates to an external third-party audit reporting application. Additional services-related costs may apply for configuration of outbound audit event data to meet the formatting constraints of any such third-party audit reporting application.	If a third-party audit reporting application is used, configuration of audit events to be securely transmitted from Millennium is required. Audit event data is captured and transmitted outbound to the audit log repository in XML format according to the Audit Trail and Node Authentication (ATNA) profile standard message structure and may be subject to customization or modification to conform to the inbound formatting requirements of any such third-party application.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2018. **Relied upon software**: ntpd (Linux)	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Use of Privacy Analytics as the audit repository and reporting application is recommended and is subject to additional licensing costs if utilized. If a certified third-party audit reporting application (e.g., Fair Warning) is used in place of Privacy Analytics, a license for the Privacy Analytics Listener is recommended (but not required).	Reporting capabilities for audit events and data from the certified product that are captured via Millennium Core Audit Service require use of an external audit repository and reporting application to which audit data is securely transmitted after capture supporting physical separation of the audit log from the HIT module that is the subject of the audit in accordance with good security practices. Privacy Analytics is recommended as the audit reporting application, but third-party applications may also be leveraged. If a third-party audit reporting application is used, implementation of the Privacy Analytics Listener is highly recommended as best practice for interfacing data from the Millennium environment to the foreign application. Without it, there is potential for communication issues with residual impact on system performance in Millennium.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed via *FirstNet* locally to end-user devices (e.g. temp files, caches). **Relied upon software**: N/A	No required costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2018. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(1) Transmission to Immunization Registries	Includes the ability to record immunizations data codified using National Drug Code (NDC) identifiers for administered vaccines and Codes for Vaccines Administered (CVX) identifiers for historical vaccines, with subsequent creation of immunization messages formatted according to HL7 and CDC standards, along with the ability to query for and access/display a patient's	Required costs include software licenses for PowerChart OR Emergency Medicine (FirstNet), Medication Administration Record, CAMM Digital Objects, and Cerner Hub – Immunizations or Vaccinations Outgoing Interface. Optional costs include the following: Cerner Point of Care and/or CareAware Connect for automated documentation of vaccine administration (including recording of NDC codes) via barcode	For interfacing with the external immunization registry, specific configuration requirements are necessary. The interfacing can be configured as either a direct point-to-point connection through Foreign System Interfaces and the reporting registry OR configured as a connection through Cerner *Hub* services for reporting immunization data to the registry. Connecting via the *Hub* for immunization query capabilities is *highly recommended* to accommodate variances and unique connection dependencies across individual IIS registries, but it is also acceptable for a client to create their own transport mechanism via an interface engine or other means capable of satisfying their IIS registry's requirements.

	immunizations history and forecast according to HL7 and CDC standards. **Relied upon software**: Cerner Hub – Immunizations OR Vaccinations Outgoing Interface	scanning, Cerner *MPages* for use of the Immunizations Workflow component, and Cerner Immunizations Registry Query (Hub) for registry query connection. If choosing to leverage barcode medication administration capabilities for recording vaccine administration with capture of National Drug Code (NDC), additional costs may apply for handheld scanner hardware. For organizations who elect to voluntarily adopt enhanced clinical reconciliation capabilities via Cerner's Seamless Exchange offering, an additional monthly subscription and associated set up fees apply. Other pre-requisite costs for Seamless Exchange capabilities include an annual subscription and one-time set up fee for Cerner's Immunizations Registry Query (Hub), and an *annual subscription and one-time set up fee for Cerner's Ignite Millennium API (for clients that host their own infrastructure (CHO), an additional one-time setup cost for additional infrastructure is required, and supplemental costs for RedHat Licenses, VMWare licenses, and ESX Host hardware may apply). *The Millennium Ignite API (the API) costs are the same as those required for the 170.315(g)(7)-(9) criteria certification under the same Certified Health IT Module (no additional fees apply if the API is already implemented for those criteria).	For the Millennium 2018.01 release platform, USB-connected scanners are required if the optional Medication Administration Wizard (MAW) is used for automated documentation of vaccine administration via barcode scanning (PS/2 scanner connections will not be compatible). Successful implementation of the certified capabilities requires configuration of the Workflow *MPages* Immunizations component or the Immunization Schedule for charting of historical vaccines. For charting of new vaccine administrations and recording of the administered NDC, vaccine pharmacy formulary details and supply chain locations where vaccines are stocked should be configured, along with enabling Lot selection in the medication administration window. Registry Import must be configured for querying the external registry to access immunization history and display forecast. Configuring the Immunization Ad Hoc preference to disable charting from Immunization Schedule is recommended, but not required. Other considerations include the following: if charting immunizations ad-hoc directly from Immunization Schedule, the system will not capture the NDC code as required for reporting; if enabling lot selection preference, the system does not allow the user to modify vaccine details after charting an administration and (user must un-chart/re-chart the administration); if a direct modification is necessary, the lot selection preference can be disabled, but Cerner intends for the preference to be enabled for inventory integration. For organizations who elect to voluntarily adopt enhanced immunization registry query capabilities via Cerner's Seamless Exchange offering, additional pre-requisites include the following: Millennium 2018.03 code base or higher, MPages version 6.16 or higher, cloud onboarding with HealtheIntent data onboarding, and Ignite API implementation with Fast Healthcare Interoperability Resources (FHIR) R4 mappings.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Patient Portal *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: Cerner Millennium	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for encrypted device and/or cloud storage of the exported data.	EHI created by the Patient Portal certified HIT module is stored in the tethered Millennium EHR system's database, which is leveraged as relied upon software for the certification. This EHI consists primarily of secure messages exchanged between the patient and their care team(s). The export is also inclusive of the full scope of data that is accessible for viewing, downloading, and/or transmitting in the Patient Portal, although that data is not stored in or by the Patient Portal. For further details on implementation pre-requisites and guidance, please refer to the 170.315(b)(10) EHI Export line item on the Millennium (Clinical) certified HIT module included in this document. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e., username/password) to gain access to electronic health information in the Patient Portal, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	N/A
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Support event creation capabilities for security auditing of access to and actions on ePHI within the Patient Portal, including integrity protection of recorded audit logs. Cures Update criterion certification available as of product version 2021. **Relied upon software**: N/A	No associated costs or fees – the security auditing capabilities provided by the cloud auditing service are considered embedded with the licensing of the Health IT module itself.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. The cloud auditing service is not able to be disabled once deployed and does not require or support management of specific events of interest to be logged as the big data foundation model follows an approach of always sending everything.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2021. **Relied upon software**: N/A	No associated costs or fees – audit reporting capabilities are available through the Privacy Analytics certified audit reporting application or via export of audit data for import to a third-party audit reporting application for no additional fees.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. Successful use of exported audit data in third-party reporting applications may require additional customization or modification of the event formatting to align with inbound formatting requirements of the third-party.
§ 170.315(d)(5) Automatic Access Time-out	Enables automatic termination of a user session after a specified period of inactivity requiring re-authentication.	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	The automatic time-out capability is subject to the specific Identity Provider (IdP) in use with the patient portal. When the default Cerner consumer IdP is in use, automatic access time-out is enabled by default and set to a standard inactivity period 20 minutes for all clients/users. Time-out settings may vary if a custom or third-party IdP is in use.

	Relied upon software: Cerner Millennium		
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information accessed in the portal locally to end-user devices (e.g., temp files, cookies, caches). **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Patient Portal prevents ePHI from being stored locally to end-user devices via "no-cache" and "no-store" headers. Use of non-recommended browsers that do not respect these headers may negatively impact the capabilities.
§ 170.315(d)(9) Trusted Connection	Enables the secure encryption and integrity-protection of electronic health information transmitted to and from the portal, including secure messages between patients and their provider, contribution of data for patient health information capture, and secure transmit of health information to a 3rd party. **Relied upon software**: Cerner Direct Messaging	Required costs beyond the licensing required for the Health IT module include a license for Cerner Direct Messaging to enable message-level trusted connection for secure transmit of health information to a 3rd party. ***NOTE** *Cerner Direct Messaging* is already a required license for the Health IT module by virtue of its support for the 170.315(e)(1) criterion	The trusted connection capabilities are included with a standard implementation of Patient Portal and unsecure transport methods for exchange of ePHI are not intended to be used or supported (except in the case of the required capability for a patient or authorized representative to transmit to any e-mail address of the patient's choice under the 170.315(e)(1) criterion). For secure data exchange in the context of patient health information capture (170.315(e)(3)) and secure messaging (170.315(e)(2)), full successful implementation is dependent upon Websphere application server (WAS) configuration including TLS v1.2 communications security and digital certificates with SHA-2 support. In the case of secure transmit of health information to a 3rd party (170.315(e)(1)), configuration of the *Cerner Direct Messaging* in the integrated Cerner Millennium environment would be required for a full successful implementation.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2021. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2021. **Relied upon software:** N/A	N/A	N/A
§ 170.315(e)(1) View, Download, and Transmit to 3rd Party	Includes the capability for patients and their authorized representatives to access their health information electronically, and download and transmit it to a 3rd party (via both secure encrypted and unencrypted methods) in a C-CDA format using the Continuity of Care Document (CCD) template. Also includes the ability to view health information associated with a specific date and/or	Required costs include software licenses for Patient Portal, PowerChart (or PowerChart Ambulatory or PowerChart ASP) or Emergency Medicine (FirstNet), CareAware MultiMedia (CAMM) Digital Objects, and Cerner Direct Messaging. For the new Patient Portal Cloud Service edition of the product available as of August 2024, additional software licenses for the updated edition and Oracle Health FHIR APIs are also required.	User access provisioning and authentication in Patient Portal requires an Identity Provider (IdP). The default IdP is the Cerner consumer IdP; use of a custom or third-party IdP is subject to pre-requisites and must conform to documented specifications available in Cerner's *Patient Portal SAML 2.0 Specification* Reference Page. For the new Patient Portal Cloud Service edition of the product available as of August 2024, use of a custom IdP will require implementation of Oracle Identity Cloud Service (IDCS). The IdP will be federated with IDCS to enable use.

	date range and access a detailed activity history log of actions in their portal. Cures Update criterion certification available as of product version 2022. **Relied upon software**: Cerner Millennium	Optional costs include licensing for the following: Advanced Interoperable Solutions (AIS) for XDR/XDM secure exchange; Cerner Registration Management or Practice Management for provision of access to patients and authorized representatives; Radiology Management for enabling access to diagnostic imaging results; General Laboratory for enabling access to laboratory results.	A mechanism for provisioning users with the IdP via invitation for patients to access to their health information in the portal must also be established. Use of Cerner registration applications is recommended and enables direct integration. If a foreign registration system is utilized, additional interfacing will be required for support of the invitation process. The following pre-requisite configurations must be in place to support view, download, and transmit to 3rd party capabilities via Patient Portal: Millennium OAuth, CareAware OAuth, CareAware MultiMedia (CAMM), Enterprise Appliance (EA) Millennium services installation (**needs may differ for client-hosted vs. remote-hosted clients*), and *Cerner Direct Messaging* (including a unique messaging address for Patient Portal). Continuity of Care Document (CCD) template(s) for patient access must also be configured in Millennium to populate all data elements required for the 170.315(e)(1) criterion, and subsequently configured as the source template(s) in the Patient Portal Administration Tool. For the new Patient Portal Cloud Service edition of the product available as of August 2024, implementation of Oracle Health FHIR APIs must also be in place. Laboratory results (and associated Labs CLIA information) interfaced inbound to Millennium from a foreign Laboratory Information System (LIS) or reference lab and diagnostic imaging results interfaced inbound from a foreign radiology/imaging system must align with standard Millennium clinical event posting to accurately populate in C-CDA documents for patient access. Availability of lab results for patient access in the portal should be configured with consideration of applicable state laws in addition to Promoting Interoperability program requirements.
§ 170.315(e)(3) Patient Health Information Capture	Includes the capability for patients or their authorized representatives to securely and electronically provide health information from non-clinical settings to providers and care team members for incorporation into their health record. **Relied upon software**: Cerner Millennium	Required costs include software licenses for Patient Portal, PowerChart (or PowerChart Ambulatory or PowerChart ASP) or Emergency Medicine (FirstNet), and Advanced Care Documentation (PowerForms) for capture of hyperlinks to patient-provided health information in the EHR.	Patient Portal's certification for Patient Health Information Capture is intended for use of Patient Portal secure messaging as the method used by patients (or their authorized representatives) to securely and electronically share health information with their providers. Providers are then able to identify the shared information upon receipt in Millennium Message Center and record it to the patient's record for subsequent access and reference. Use of an application other than Patient Portal as the contributing source would not be considered valid under Patient Portal's certification. Capture of patient-provided hyperlinks to patient health information is performed directly in the tethered Millennium EHR using a select PowerForm. To enable messaging capabilities for individual users, providers must be set up with a messaging feature associated to their Millennium HNA user account, and patients/authorized representatives must have an active Patient Portal account. *Millennium (Clinical) is also certified to the criterion and enable connecting with patient portals and applications other than Patient Portal as contributing sources
§ 170.315(g)(2) Automated Measure Calculation Note – this criterion applies exclusively to the version 2024 listing of this certified HIT module. Version 1 of the product is	Enables calculation of numerator and denominator values for the following Stage 3 Promoting Interoperability (PI) measures for performance/reporting year 2019+: Medicare PI • Provide Patients Electronic Access to Their Health Information (EH/CAH & EC) Medicaid PI (EP only) • Patient Electronic Access	Required costs include software licenses for Patient Portal, PowerChart (or PowerChart Ambulatory or PowerChart ASP) or Emergency Medicine (FirstNet), and Business Objects.	Standard functional reports for automated measure calculation are designed to work in coordination with certified product capabilities and workflows. Information on the design assumptions of the reports is available in Cerner Reference Pages documentation. Use of self-developed components or use of workflows that are beyond the scope of the design assumptions of the standard reporting may not result in measurement consideration. Use of self-developed reporting or process to compile numerator and denominator data from different sources than the certified product is outside the scope of Cerner's certified capabilities.

able to support Promoting Interoperability functional reporting via utilization of the separate *HealtheAnalytics: Promoting Interoperability* certified HIT module.	• Patient Education • View, Download, Transmit • Secure Messaging • Patient Generated Health Data **Relied upon software**: N/A		To enable the certified capability to be used configuration in the Cerner *Bedrock* wizard for definition of denominator populations and for measure definitions is required. Operations processes must also be implemented to support data loads for the reporting period. If reporting requirements change because of CMS policy clarifications or due to identification of error correction needs in reporting logic, this can require historical loads of data to assure proper measure calculation and credit.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(6) C-CDA Creation Performance	Enables the creation of a standards-conformant Consolidated Clinical Document Architecture (C-CDA) document, including Common Clinical Data Set (CCDS) representation. Cures Update criterion certification available as of product version 2022. **Relied upon software**: N/A	Required costs beyond the licensing required for the Health IT module include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP) or Emergency Medicine (FirstNet).	The C-CDA creation performance capabilities are supported as per ONC policy with the 170.315(e)(1) certification for creation of a C-CDA document for patient view, download, and transmit of health information using the CCD template. Capabilities native to *PowerChart* and *FirstNet* in Cerner Millennium are leveraged as relied upon software for the C-CDA generation. Appropriate implementation and maintenance of medical code sets for vocabulary constraints and mapping of demographics data elements to defined standards is a pre-requisite for conformant C-CDA generation. For the Implantable Device List included in the Medical Equipment section of C-CDA documents, device entries with a UDI and a status of active (i.e. currently implanted) are included in the C-CDA. An additional enhancement to populate active Implant History entries *without* a UDI is also available for all certified code levels.

PowerChart Touch *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(a)(1) Computerized Physician Order Entry (CPOE) – Medications	Includes the capability to electronically record, change, and access a patient's medication orders. **Relied upon software**: Cerner Millennium	Required costs include software licenses for Mobility Extension for Physician (PowerChart Touch), PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders, and a Multum content subscription. Ongoing support costs are required based on the solution licenses.	As part of the appropriate use of the certified capability, clients are expected to maintain currency with *Multum* content updates to have accurate reflection of the current RxNorm code set. Use of Cerner-provided ancillary department ordering conversations, such as are available within *PharmNet*, are not considered to be within scope of the certified capabilities. Availability of medication orders for CPOE requires configuration and ongoing maintenance of a pharmacy order catalog and appropriate role-based security on the connected Millennium desktop environment.
§ 170.315(a)(2) Computerized Physician Order Entry (CPOE) – Laboratory	Includes the capability to electronically record, change, and access a patient's laboratory orders. **Relied upon software**: Cerner Millennium	Required costs include software licenses for Mobility Extension for Physician (PowerChart Touch), PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders. Ongoing support costs are required based on the solution licenses.	Use of Cerner-provided ancillary departmental ordering conversations, such as are available within *PathNet*, are not considered to be within scope of the certified capabilities. Availability of laboratory orders for CPOE requires configuration and ongoing maintenance of a laboratory order catalog and appropriate role-based security on the connected Millennium desktop environment.
§ 170.315(a)(3) Computerized Physician Order Entry (CPOE) – Diagnostic Imaging	Includes the capability to electronically record, change, and access a patient's diagnostic imaging orders. **Relied upon software**: Cerner Millennium	Required costs include software licenses for Mobility Extension for Physician (PowerChart Touch), PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders. Ongoing support costs are required based on the solution licenses.	Use of Cerner-provided ancillary departmental ordering conversations, such as are available within *RadNet*, are not considered to be within scope of the certified capabilities. Availability of diagnostic imaging orders for CPOE requires configuration and ongoing maintenance of an imaging order catalog and appropriate role-based security.
§ 170.315(a)(4) Drug-drug, Drug-Allergy Interaction Checks for CPOE	Includes the capability to detect and alert end-users of drug-drug and drug-allergy interactions when placing medication orders, and the ability to manage the severity level by which interaction alerts are triggered. **Relied upon software**: N/A	Required costs include software licenses for Mobility Extension for Physician (PowerChart Touch), PowerChart (or PowerChart Ambulatory or PowerChart ASP) and PowerOrders, and a Multum content subscription for mCDS.	As part of the appropriate use of the certified capability, clients are expected to maintain currency with *Multum* content updates to have accurate reflection of the current RxNorm code set and drug-drug/drug/allergy interaction content, including reference sources. Use of other *Multum* content is outside the scope of the certified capabilities. Successful implementation of the certified capabilities requires Multum content installation and enabling of preferences for drug-drug/drug-allergy interaction checking. Clients can configure preferences to fit their individual policies for alert levels (e.g. moderate, major, contraindicated, etc.). Drug-allergy interaction checking is not supported for inactive ingredients that may be included in medications (e.g., food-based ingredients) or IV solution base components (e.g., dextrose, sodium chloride, etc.). Full details are published in Cerner's *Managing Cerner Multum Content* Reference Page.
§ 170.315(b)(3) Electronic Prescribing	Includes the capability to transmit and receive prescription messages according to National Council for Prescription Drug Programs' (NCPDP) 2017071 standard, including for New, Change, Cancel, Refill, Fill Status, and Medication History transaction, along with enforcing leading/trailing zeros logic and mL dosing units for oral liquid medications. **Relied upon software**: Cerner Millennium	Required costs include software licenses for Mobility Extension for Physician (PowerChart Touch), PowerChart (or PowerChart Ambulatory or PowerChart ASP), PowerOrders, Cerner ePrescribe, and a Multum content subscription. For client-hosted (CHO) clients, additional costs for a VPN solution to securely connect the desktop Millennium environment to Cerner's ePrescribing Hub may apply.	To transact on the Surescripts electronic prescribing network, prescribers must be registered with Surescripts and obtain an SPI (Surescripts Provider ID). The certified capability includes notification alert messages to providers for electronic prescription failures. If the transmission of a prescription order to a pharmacy fails, a routing error message is sent to either the ordering provider's Message Center or their designate (pool). In addition to Surescripts pre-requisites, successful implementation and use of the certified capabilities requires that a provider's demographic information (address, phone, fax, identifiers) be

			configured in the Millennium environment. Millennium pharmacy order catalog (including *Multum* content updates) must also be maintained to reflect the commercial availability of prescription products. ePrescribe transactions supported natively from the *PowerChart Touch* application are isolated to New and Cancel Prescription message types. All additional message types require use of workflows within *PowerChart* on the connected Millennium desktop environment. *PowerChart Touch* also supports ePrescribing for Ambulatory encounters exclusively; support for Inpatient encounters requires use of *PowerChart* workflows on the connected Millennium desktop environment.
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: Cerner Millennium	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for encrypted device and/or cloud storage of the exported data.	EHI created by the PowerChart Touch certified HIT module is stored in the tethered Millennium EHR system's database, which is leveraged as relied upon software for the certification. For further details on implementation pre-requisites and guidance, please refer to the 170.315(b)(10) EHI Export line item on the Millennium (Clinical) certified HIT module included in this document. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to electronic health information in the *PowerChart Touch* application, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: Cerner Millennium	Required costs beyond the licensing required for the Health IT module include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP).	Cerner's *Millennium OpenID* Provider is utilized to securely integrate Millennium user identities (HNA accounts with associated credentials and security privileges) to the *PowerChart Touch* application's cloud-based architecture. Given the *Millennium OpenID* Provider's unique integration with the underlying Millennium credentials, use of any third-party or custom identity management service is not enabled. Configuration of user accounts with associated security privileges, authentication parameters, and related access controls is required for use of the certified capability. The *Millennium OpenID* Provider requires pre-requisite configurations, including installation of the Millennium Identity server and OAuth registration. Additional network dependencies detailed on Cerner's *Millennium OpenID Provider Overview* Reference Page may apply. Individual devices used for accessing the *PowerChart Touch* application must also be provisioned through Cerner's Device Access framework using a unique access code generated by IT staff for the initial login. Without a valid provision, users cannot access the application. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of access to and actions on ePHI within the *PowerChart Touch* application, including integrity protection of recorded audit logs. Cures Update criterion certification available as of product version 4. **Relied upon software**: *N/A*	No associated costs or fees – the security auditing capabilities provided by the cloud auditing service are considered embedded with the licensing of the Health IT module itself.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. The cloud auditing service is not able to be disabled once deployed and does not require or support management of specific events of interest to be logged as the big data foundation model follows an approach of always sending everything.

§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 4. **Relied upon software**: *N/A*	No associated costs or fees – audit reporting capabilities are available through the Privacy Analytics certified audit reporting application or via export of audit data for import to a third-party audit reporting application for no additional fees.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. Successful use of exported audit data in third-party reporting applications may require additional customization or modification of the event formatting to align with inbound formatting requirements of the third-party.
§ 170.315(d)(4) Amendments	Enables recording of patient requests for amendment to their health record, including identification of whether the amendment was approved or denied. **Relied upon software**: Cerner Millennium	Required costs beyond the licensing required for the Health IT module include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP).	Use of capabilities within the connected Millennium desktop environment for which the *PowerChart (Clinical)* module is certified for enable the capabilities for this criterion. It is assumed that client definition and use of amendment capabilities should be flexible based on their form and manner of recording patient requested amendments. Amendments of ePHI maintained in non-certified systems is beyond the scope of Cerner's certified capability but Cerner recognizes they may be in use for maintenance of ePHI beyond the scope of records maintained by the certified system. Documentation templates can be defined both for recording patient requests/provider response and for the substance of the amendment request content. Accepting the amendment request into the record may involve use of additional documentation tools to create and maintain medical record entries out of amendment requests, such as for documenting a patient's home medications or recording patient contributed health information, depending on its form.
§ 170.315(d)(5) Automatic Access Time-out	Enables automatic termination of a user session after a specified period of inactivity requiring re-authentication. **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Cerner mobile applications invoke automatic log-off at a session inactivity period of 900 seconds (15 minutes) by default. This setting can be modified to a value less than or equal to the maximum session duration as desired and can also be configured to differ for personal and shared provisions.
§ 170.315(d)(6) Emergency Access	Enables a limited set of specified users to access electronic health information in emergency scenarios. **Relied upon software**: Cerner Millennium	Required costs beyond the licensing required for the Health IT module include a software license for PowerChart (or PowerChart Ambulatory or PowerChart ASP).	Use of capabilities within the connected Millennium desktop environment for which the PowerChart (Clinical) product is certified for enable the capabilities for this criterion. Use of business continuity and disaster recovery techniques and tools are beyond the scope of the intent of emergency access capabilities within the certified product but are relevant for HIPAA Security compliance and overall security risk assessment processes. To enable the certified capability to be used, configuration of user positions with privilege to invoke the emergency access relationship type must be defined. This capability allows for override of restrictions on a user's ability to access records beyond the organization they are associated to, of encounter records marked as subject to confidentiality levels and based upon the access rights that may be defined for the emergency mode of access relationship type.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information accessed in the *PowerChart Touch* application locally to end-user devices (e.g. temp files, cookies, caches). **Relied upon software**: N/A	No associated costs or fees – the capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
§ 170.315(d)(8) Integrity	Enables verification that health information exchanged electronically (both outbound and inbound) has not been altered during transmit via use of message digests produced by hash algorithms of SHA-2 or greater strength.	Required costs beyond the licensing required for the Health IT module include software licenses for PowerChart (or PowerChart Ambulatory or PowerChart ASP) and Cerner Direct Messaging.	Use of capabilities within the connected Millennium desktop environment for which the PowerChart (Clinical) product is certified for enable the capabilities for this criterion. Integrity protection is enabled principally for secure transport of clinical information between entities for those end points and transacting capabilities intended for use with the certified Health

	Relied upon software: Cerner Millennium	***NOTE** Cerner Direct Messaging is already a required license for the PowerChart (Clinical) Health IT module relied upon for this criterion by virtue of its support for the 170.315(h)(1) criterion	IT module. Unsecure transport methods for ePHI between entities may lead to risk of security vulnerability and are not recommended. Use of the certified capability requires full implementation and onboarding of the Cerner Direct Messaging for the given Millennium environment.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 4. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 4. **Relied upon software:** N/A	N/A	N/A
§ 170.315(g)(2) Automated Measure Calculation	Enables calculation of numerator and denominator values for the following Stage 3 Promoting Interoperability (PI) measures for performance/reporting year 2019+: Medicare PI • e-Prescribing (EH/CAH & EC) • Verify Opioid Treatment Agreement (EH/CAH only) Medicaid PI (EP only) • ePrescribing • CPOE **Relied upon software**: Cerner Millennium	Required costs include software licenses for Mobility Extension for Physician (PowerChart Touch), PowerChart (or PowerChart Ambulatory or PowerChart ASP), and Business Objects.	Standard functional reports for automated measure calculation are designed to work in coordination with certified product capabilities and workflows. Information on the design assumptions of the reports is available in Cerner Reference Pages documentation. Use of self-developed components or use of workflows that are beyond the scope of the design assumptions of the standard reporting may not result in measurement consideration. Use of self-developed reporting or process to compile numerator and denominator data from different sources than the certified product is outside scope of Cerner's certified capabilities. To enable the certified capability to be used configuration in the Cerner Bedrock wizard for definition of denominator populations and for measure definitions is required. Operations processes must also be implemented to support data loads for the reporting period. If reporting requirements change because of CMS policy clarifications or due to identification of error correction needs in reporting logic, this can require historical loads of data to assure proper measure calculation and credit.
§ 170.315(g)(3) Safety Enhanced Design	Defines user-centered design processes and assessments for applicable certified capabilities within the certified product's scope. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained.	No associated costs or fees	N/A

	Relied upon software: N/A		
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Privacy Analytics *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2021. **Relied upon software**: N/A	Required costs include license rights for Privacy Analytics. For the Software as a Service (SaaS) model, license rights are subscription-based and recurring fees are subject to increase if data ingestion volume exceeds contracted amount. If transitioning from traditional installed software solution model to SaaS, optional services for migration of audit trail data are subject to additional fees. Optional costs may apply for inbound configuration of audit events to post to Privacy Analytics that may come from non-Cerner source systems.	Privacy Analytics is intended for use with Cerner Millennium-based clinical systems but non-Cerner source clinical solutions (including non-certified systems and applications) can also send audit data to Privacy Analytics if leveraging the traditional installed software solution model. Non-Millennium data sources are not currently supported on the Privacy Analytics SaaS model. Standard reporting capabilities of Privacy Analytics are included for all clients. Any other reporting capabilities desired beyond those enabled via the standard reporting may be subject to client configuration or assistance by Cerner Consulting Associates.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Syndromic Surveillance and eLab Results *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(d)(1) Authentication, Access Control, Authorization	Supports unique user identification, enables authentication against unique identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Configuration of user accounts with associated security privileges, authentication parameters, and related access controls is required for use of the certified capability. Use of any advanced authentication methodologies, such as biometrics or cryptographic methods used in two-factor authentication, are beyond the scope of certified product capabilities. Similarly, use of any external authentication methods that are pass-through to the certified product's security services or external directory services for user account/credential management are beyond the scope of the certified capabilities.
§ 170.315(d)(2) Auditable Events and Tamper-Resistance	Supports event creation capabilities for security auditing of processing and disclosure of ePHI by the *Syndromic Surveillance* application, including integrity protection of recorded audit logs. Cures Update criterion certification available as of product version 2021. **Relied upon software**: N/A	No associated costs or fees – the security auditing capabilities provided by the cloud auditing service are considered embedded with the licensing of the Health IT module itself.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. The cloud auditing service is not able to be disabled once deployed and does not require or support management of specific events of interest to be logged as the big data foundation model follows an approach of always sending everything.
§ 170.315(d)(3) Audit Report(s)	Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. Cures Update criterion certification available as of product version 2021. **Relied upon software**: N/A	No associated costs or fees – audit reporting capabilities are available through the Privacy Analytics certified audit reporting application or via export of audit data for import to a third-party audit reporting application for no additional fees.	Audit reports are made available by default in the Privacy Analytics certified audit reporting application. Access to the application requires Cerner Cloud account set up, which can be managed at an enterprise level. Organizations wishing to send their audit data to a third-party reporting application or repository can leverage secure export capabilities which can be set up pursuant to a request. Successful use of exported audit data in third-party reporting applications may require additional customization or modification of the event formatting to align with inbound formatting requirements of the third-party.
§ 170.315(d)(7) End-user Device Encryption	The certified product is designed to prevent any persistent storage of electronic health information processed via the *Syndromic Surveillance* application locally to end-user devices (e.g. temp files, cookies, caches). **Relied upon software**: N/A	No associated costs or fees – The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Storage of data locally on end-user devices is not utilized by the applications and capabilities within scope of the certified product. Encryption capabilities for server-side or data center hosting and ad hoc user actions to export ePHI for local/personalized storage is beyond the scope of certification testing for the criterion.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. Certification available as of product version 2021. **Relied upon software:** N/A	N/A	N/A

170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. Certification available as of product version 2021. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(2) Transmission to Public Health Agencies — Syndromic Surveillance	Enables creation and transmission of public health surveillance data to external public health agencies formatted according to the HL7 2.5.1 standards for Syndromic Surveillance. **Relied upon software**: N/A	Required costs include software licenses for PowerChart or Emergency Medicine (FirstNet) and Cerner Enterprise Registration or Revenue Cycle, or an Interface from a third-party registration system, are required costs. Both set up fees and support services are also required for Syndromic Surveillance. Optional costs include custom quotes for ADT Pass Through configuration for clients using a third-party registration system and data services connections to additional public health agencies.	To enable the certified capability to be used, a data feed must be configured for interfacing from Cerner Millennium to the Syndromic Surveillance product application. If Admission/Discharge/Transfer (ADT) or observation result unsolicited interfaces from a third-party registration system into Cerner Millennium are being utilized, they *must* include all required data elements as outlined by Centers for Disease Control and Prevention implementation guides for Cerner to begin the Syndromic Surveillance build. Additionally, A01, A03, A04, and A08 ADT triggers *must* be enabled.
§ 170.315(f)(3) Transmission to Public Health Agencies — Reportable Laboratory Tests and Value/Results	Enables creation and transmission of laboratory tests and results data for external reporting to public health agencies formatted according to the HL7 2.5.1 standards for Electronic Laboratory Reporting to Public Health. **Relied upon software**: N/A	Required costs include software licenses for General Laboratory and Microbiology (unique Microbiology license only required if discrete micro results are not supported via Gen Lab). Both set up fees and support services are also required for Electronic Lab Results, along with LOINC and SNOMED-CT content for codified result data. Optional costs include professional services for LOINC code assignment and data services connections to additional public health agencies.	To enable the certified capability to be used, *PathNet* data feed must be configured for the submission of data to the *Electronic Lab Results* application, and onboarding activities with local or state public health jurisdiction completed, including registration of intent. LOINC and SNOMED-CT mapping for laboratory reportable conditions in Cerner Millennium is also required. LOINC codes must be present at both orderable and result level in Cerner Millennium and a content package must be installed prior to implementation for SNOMED-CT mappings. Any additional SNOMED-CT codes required by the public health registry for submission that are not included in the pre-requisite content package can be accommodated by Cerner via assignment in the *Electronic Lab Results* application directly.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	No associated costs or fees	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	No associated costs or fees	N/A

Soarian Clinicals Certified Health IT Modules

Soarian Clinicals

See Appendix A for certified versions and CHPL listing information. See Appendix B for comprehensive list of certified Clinical Quality Measures.

The Soarian Clinicals certified module consists of software branded as Soarian Clinicals, Pharmacy, Med Administration Check, ePrescribing, Advanced Interoperability Service (AIS), Cerner OPENLink, Ignite Soarian API, Health Services Analytics (Soarian Quality Reporting Service (SQRS) or Healthcare Intelligence- Clinical Intelligence (CI) and Healthcare Intelligence- Quality Measures Intelligence (QMI) or Decision Support Solutions (DSS) and Soarian Quality Measures (SQM) and Healthcare Query (HQ)).

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(a)(1) CPOE Medications	CPOE Medications (Order, Change, and Access) applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs. Includes the capability to electronically record, change, and access a patient's medication orders. **Relied upon software**: To utilize RxNorm code set for ordered medications in other capabilities such as eCQM calculation, a license for FDB's Enhanced Interoperability Module is required.	A Soarian Clinicals software license and standard First Data Bank (FDB) content (which is included) is required. To enable the certified capability to be used, standard CPOE implementation including configuration of medication orders is required to enable order entry. Costs may apply for optional implementation services.	As to the intended use of certified capability it is assumed that clients are expected to maintain currency with software and content updates. Standard implementation for medication orders includes Pharmacy implementation but this is out of scope of the certified capability for order entry. Use of transactions with departmental/ancillary systems are part of standard ordering implementation but are not considered within scope of certified capability.
§ 170.315(a)(2) CPOE Laboratory	CPOE Laboratory (Order, Change, and Access) applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs. Includes the capability to electronically record, change, and access a patient's laboratory orders. **Relied upon software**: N/A	This is included in the Soarian Clinicals certified module. A Soarian Clinicals software license is required. To enable the certified capability to be used, standard CPOE implementation including configuration of laboratory orders is required to enable order entry. Costs may apply for optional implementation services.	As to the intended use of certified capability it is assumed that clients are expected to maintain software currency. Standard implementation for orders may include interface implementation with ancillary systems but this is out of scope of the certified capability for order entry. Use of transactions with departmental/ancillary systems are part of standard order implementation but are not considered within scope of certified capability. Implementation of specific code sets for ordered tests for use in other capabilities such as eCQM calculation may be required outside the scope of order entry.
§ 170.315(a)(3) CPOE Diagnostic Imaging	CPOE Diagnostic Imaging (Order, Change, and Access) applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state. Includes the capability to electronically record, change, and access a patient's diagnostic imaging orders. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A Soarian Clinicals software license is required. To enable the certified capability to be used, standard CPOE implementation including configuration of diagnostic imaging orders is required to enable order entry. Costs may apply for optional implementation services.	As to the intended use of certified capability it is assumed that clients are expected to maintain software currency. Standard implementation for orders may include interface implementation with ancillary systems but this is out of scope of the certified capability for order entry. Use of transactions with departmental/ancillary systems are part of standard order implementation but are not considered within scope of certified capability. Implementation of specific code sets for ordered tests for use in other capabilities such as eCQM calculation may be required outside the scope of order entry.
§ 170.315(a)(4) CPOE Drug-Drug, Drug-Allergy Interaction Checks	Drug-Drug, Drug-Allergy (DD/DA) Interaction Checks applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including clinical decision support for interaction checking during CPOE Medications. Includes the capability to detect and alert end-users of drug-drug and drug-allergy interactions when placing medication orders, and the ability to manage the severity level by which interaction alerts are triggered.	A Soarian Clinicals software license and standard First Data Bank (FDB) content (which is included) is required. To enable the certified capability to be used, drug-drug/drug-allergy interaction checking is configurable by the client to fit their policy for the level of alerting (e.g. low, high). Costs may apply for optional implementation services.	As to the intended use of certified capability it is assumed that clients are expected to maintain currency with software and content updates. Use of FDB content integrated with CPOE for drug-drug/drug-allergy interaction checking - use of other content is outside the scope of certified product capability. Drug-drug/drug-allergy interaction checking during clinical information reconciliation requires a license for FDB's Enhanced Interoperability Module for use of RxNorm coded content; this capability is outside the scope of this certification criterion.

	Relied upon software: N/A		
§ 170.315(a)(5) Demographics	Demographics applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and contributes to those Objectives that utilize this data such as patient engagement, coordination of care, public health (syndromic surveillance), as well as quality measure reporting (eCQM) capture and calculation. Includes the capability to electronically record, change, and access certain patient demographics – including race & ethnicity, preferred language, birth sex, and sexual orientation & gender identity – in accordance with defined vocabulary standards & code sets. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A software license is required for Soarian Clinicals. Optional costs are Inbound ADT interface and Outbound ADT Interface and available implementation services. Costs may apply for available optional implementation services.	To enable the certified capability to be used, mapping may be required to go from local codes that are used in registration conversations to the required vocabulary standards. Current conversations may need to be updated to allow for multiple responses and options to decline to specify or unknown. As to the intended use of certified capability, it is assumed that required code set values may not need to be natively captured in registration conversations within Cerner, but mapping should be in place to support outbound interfacing purposes such as for the C-CDA. Non-Cerner registration conversations can be used if the information is interfaced in to the system, but those non-certified components might not support use of the required code sets or enable multi-response to questions for race and ethnicity. An inbound interface also should be evaluated for its ability to support all related capabilities including translating and mapping the inbound code set values to required code set values if necessary. The 2015 Edition introduces into this criterion elements for Sexual Orientation and Gender Identity which may be captured at registration or captured in clinical documentation; however, these elements are not required to be captured for Meaningful Use. To enable this capability, ADT fields are provided and are available to Provider Documentation and Nursing. If configured, codes for these elements would be established in ADT implementation.
§ 170.315(a)(9) Clinical Decision Support	Clinical Decision Support (CDS) applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition. Includes the capability to configure CDS interventions inclusive of source attribute information to be presented to end-users based on clinical data in the Electronic Health Record (EHR), along with retrieval of diagnostic and therapeutic reference information using the Infobutton standard. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A Soarian Clinicals software license is required.	As to the intended use of certified capability it is assumed that Clients are expected to ensure drug-drug, drug-allergy checking and other clinical decision support capabilities are enabled as needed in their clinical practice. Active use of the Infobutton retrieval capability requires integration of external content that adheres to the URL-based implementation of the Infobutton standard, which may require contracting with third-party vendors. Where applicable, clients are responsible for ensuring CDS interventions are enabled and maintained for the duration of anyPromoting Interoperability reporting period. Standard content is available for optional use at no cost for rules-based CDS. Clients are not required to utilize rules or standard content in pursuit of CDS and may use alternate means within CMS CDS guidance and the capabilities of the certified modules such as order entry, clinical documentation automation, patient education suggestion via Infobutton, and other means described in solution documentation.
§ 170.315(a)(12) Family Health History	Family Health History Status applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition. Includes the capability to electronically record, change, and access a patient's family health history using SNOMED-CT vocabulary for documented conditions. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A Soarian Clinicals software license is required.	As to the intended use of certified capability it is assumed that clients are expected to maintain currency with software and content updates. To enable the certified capability to be used SNOMED-CT may need to be mapped to existing values used for clinical documentation, if different. Codified values are managed in Soarian Content Management Workspace (SCMW). As part of a required implementation service, new SCMW model content will be published enabling the use of codified values. Training is required for SCMW.
§ 170.315(a)(14) Implantable Device List	Implantable Device List applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives that utilize this data such as patient engagement and coordination of care. Includes the capability to manage a list of a patient's implantable devices, including recording and parsing Unique Device Identifiers (UDI) and to support automated retrieval	This is included with the Soarian Clinicals certified modules. A Soarian Clinicals software license is required. Optional advisory and implementation services are available. Barcode scanner hardware are optional costs for automated recording/parsing of Unique Device Identifiers (UDI) via barcode scanning.	As to the intended use of certified capability it is assumed that clients are expected to maintain currency with software and content updates. This criterion includes the capability to chart implantable devices with Unique Device Identifiers (UDIs), including parsing the UDI, capturing key data about the device from Food and Drug Administration's Global UDI Database (FDA GUDID), and including UDI information in a consolidated clinical documentation architecture document (C-CDA). Capture and integration of this information from the point of care is not within the scope of the criterion. To enable the certified capability a compatible bar code scanner is optional and recommended. Integration of a

	of additional device attributes from the Global Unique Device Identifier Database (GUDID). **Relied upon software**: N/A		web service call to the FDA GUDID is required for accessing additional information about the UDI is part of a required implementation service.
§ 170.315(b)(1) Transitions of Care	Transitions of Care applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives for coordination of care among providers. Capabilities include the creation of C-CDAs, the sending and receiving of C-CDAs via secure edge protocols, validating C-CDAs received, and configuration of viewing preferences. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A software license for Soarian Clinicals including the capabilities for capturing source data for the summary of care (e.g., demographics, allergies, medications, problems, UDI, results receipt, etc.) is required including an Advanced Interoperability Service (AIS) subscription.	Code sets for generation and/or validation may require licensing from their source. Code sets from original sources are used for inbound verification: LOINC and UCUM: Regenstrief Institute, Inc, RxNorm: National Library of Medicine (NLM), Department of Health and Human Services (HHS), SNOMED-CT: UMLS Metathesaurus NLM HHS, ICD-9, ICD-10: Centers for Medicare and Medicaid Services (CMS), HL-7 Terminologies: HL7. As to the intended use of certified capability it is assumed that exchange is based upon use of the ONC Applicability Statement on Secure Health Transport (reference 170.315(h)(1) or (h)(2)) or XDR. With modified Stage 2 and Stage 3 measure definitions, CMS indicated that other secure electronic methods of transport beyond certified capabilities may be used and count for purpose of measurement. Non-certified exchange is beyond the scope of model product delivery and, per product documentation defining measures, may not count appropriately for the measure. Point to point XDR integration and/or XDR to HISP (reference 170.315(h)(1)) integration may be required and requires Cerner engagement. Each client must evaluate their specific exchange partners and associated communication needs. To enable the certified capability to be used these configurations should be considered; each exchange partner's secure transport method should be evaluated, integration testing performed to ensure reasonable expectation of receipt, provider-provider group addresses should be established, and processes established for inbound document handling. Viewing of C-CDA documents from outside the organization may require clients to either through purchase or through contracted licensing have the appropriate document exchange structure that allows the product to query for patient's external documents. This may be through a regional or organization owned HIE, or participation in CommonWell. Discharge Medication Reconciliation capability should be used for medication list incorporation in summary of care documentation. To enable the certified capability to be used, clinical letter module is used to produce the summary adjunct to the patient departure process. The summary of care may be automatically generated using the available generation service and rules/workflow. Soarian Communication Services (SCS) is required for sending summary of care to intended recipients from the EMR. To enable the certified capability to be used, these configurations should be considered; process updates and configuration for complete summary of care generation including required code sets, each exchange partner's secure transport method should be evaluated, integration testing performed to ensure reasonable expectation of receipt, process for discharge with transfer/referral indication, provider / provider group addresses should be established, processes established for inbound and outbound document handling, and configuration of AIS viewer and administration console.
§ 170.315(b)(2) Clinical Information Reconciliation and Incorporation	Clinical Information Reconciliation (CIR) applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives for coordination of care among providers. Includes the capability to accurately match a received transition of care C-CDA document to a local patient record and to reconcile problems, medications, and medication allergies data to produce a single consolidated reconciled list in the patient's Electronic Health Record (EHR) that can be included in subsequently generated transition of care C-CDA documents. **Relied upon software**: FDB's Enhanced Interoperability Module license is required if	This is included with the Soarian Clinicals certified modules. A software license for the Soarian Clinicals is required. An AIS subscription and integration is required for this certified capability. A C-CDA management and clinical information reconciliation implementation is required. In addition, an AIS 2015 Edition Standards for Healthcare Information Exchange is required for patient matching.	Clients are expected to stay current on software and codes / content for medications, allergies, and problems. Reconciliation of medication history from sources other than the C-CDA is not part of the scope of this criterion, but in the practice of medication reconciliation, Medication History and Surescripts subscription is optional and recommended for external Pharmacy sources of medications. Validation of inbound C-CDAs and protocols for electronic receipt of outside documents are outside the scope of this capability (reference 170.315(b)(1)).

	RxNorm coded content mapping is utilized from inbound summary of care sources to ensure inbound medications appear structured vs. free text for ease of reconciliation.		
§ 170.315(b)(3) Electronic Prescribing	Electronic Prescribing applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives for generating and transmitting permissible electronic prescriptions. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A software license for Soarian Clinicals is required, including an ePrescribing and Surecripts subscription. Cloud service integration is required (HDX).	To enable the certified capability to be used the provider should be registered with Surescripts, the Pharmacy Directory properly implemented, provider NPI/DEA configured in the EMR, and Formulary checking (reference 170.315(a)(10)) properly implemented. As part of a required implementation service, Cerner will update the medication history consent standard. Surescripts transaction notification support from Cerner and controlled substance prescribing capabilities are optional and recommended.
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. Organizations may incur ancillary costs for use of the patient population export for encrypted device(s), local network and/or (ultimately) cloud storage of the exported data.	The single patient EHI Export capability minimally requires Soarian Clinicals Version 4.5.200 EP24 or 4.6100 EP14. If RxMAK is installed, RxMAK Release 4.5.200 or above is needed. RHO clients using the Single Patient Export must use a Cerner FTP site for the exported data. This is optional but recommended for CHO clients. If the client doesn't have a Cerner FTP account, 2 eService Tickets must be opened. Instructions are documented in the *Soarian Clinicals Configuration Manual - Setting Up Electronic Health Information Single Patient Export*. CHO clients who want to perform the Patient Population Export need to ensure they have a server or external drive with enough space to copy the Soarian Clinicals data. Once the data is copied, an eService request needs to be opened to Soarian_Clinical_FHIR_ProductSupport to remove Intellectual Property (IP). Cerner will then remove the IP on the client's environment. CHO clients who have RxMAK should use the All Patient Export process to export Pharmacy data. The process is documented in *the Pharmacy and Med Administration Check EHI Export and Historical Purge Process*. RHO Clients who want to perform the Patient Population Export from Soarian Clinicals must open an eService Request to Soarian Clinicals FHIR Support requesting that all patient's data be extracted. Additionally, a Federal Information Processing Standards (FIPS) 140-2 Universal Serial Bus (USB) drive must be sent to Cerner for the purpose of copying the data. Cerner will then send that device back to the client after copying the data and removing all IP. RHO clients who have RxMAK will additionally need to open an eService request to Soarian_Clinical_FHIR_ProductSupport requesting that all RxMAK patients be extracted. Cerner exports the Pharmacy and Med Administration Check table data to XML files, which are compressed to one ZIP file and can be retrieved using the File Access published app. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(b)(11) Decision Support Interventions	Supports ability to select evidence-based and predictive decision support interventions (DSI) to deploy as part of the EHR system, along with end-user access to extensive reference information (source attributes) about DSIs supplied as part of the certified EHR and to record and export real-time electronic feedback about DSIs they're presented with in workflow. **Relied upon software:** Atlassian Confluence	Required costs include software licenses for Soarian Clinicals which includes an extended support fee for calendar year 2025. Additional costs may apply if customers choose to integrate separate collaboration software to support the requirements of the DSI criterion, but such costs would not be directly imposed by Cerner.	For enabling use of the certified capabilities Cerner recommends that Soarian Clinicals customers install third-party collaboration software, such as Atlassian Confluence or Microsoft SharePoint to integrate with the certified health IT module. Such collaboration software inherently supports attribute documentation, electronic feedback (comments), and role-based permissions for recording, updating, and editing DSI source attributes content. This can be done by using the External Application Configuration feature in Soarian Clinicals to integrate Soarian Clinicals and the chosen collaboration software. While customers can choose any collaboration software that supports the requirements, Cerner has implemented a Confluence Space that is tailored to specifically meet the DSI requirements. Customers that currently use Confluence or who choose to acquire a Confluence account from Atlassian can download a file from the Soarian_Clinicals section of Distributions. This file can be

			imported into the customer's Confluence site to create the Soarian space. This space contains the following items: • Detailed instructions for use • Soarian Clinicals model DSI attribute definitions • A template for customers to create their own DSI definitions
§ 170.315(c)(1) CQM - Record & Export	CQM Record & Export supports the Promoting Interoperability definition and IPPS/ IQR program requirement for utilization of CEHRT for eCQMs. Includes the capability to record the data required for Clinical Quality Measure (CQM) calculations in a codified manner appropriate for the measures to which the product is certified, and the ability for an authorized user to generate QRDA Category I data files for export. **Relied upon software**: Health Services Analytics	This is included in the Soarian Clinicals certified modules utilizing the Health Services Analytics component. A software license for Soarian Clinicals is required. A software license to the Health Services Analytics components is required. CMS may change eCQM definitions and submission requirements from time to time and those changes may require software, configuration, and/or process updates which may incur optional or required costs.	Health Services Analytics has brand names including SQRS or Healthcare Intelligence including Clinical Intelligence and Quality Measures Intelligence, or DSS and SQM and Healthcare Query. Codified values are managed in the SCMW. New model content including the codified values required for eCQMs is required. If clients are using 3rd party vendor data warehouse products for e-submission, they are not relying on our certified capability but relying on third party capabilities to meet the 170.315(c)(1)-(3) criteria, and are likely using custom extracts required by that third party data warehouse for exporting data from the source clinical EHR by a non-certified capability. To enable the certified capability to be used, configuration should be considered such as; configuration of reference build to map clinical data to the standard value sets, additional reference data build to support EH reporting, FDB Interoperability Module licensing for RxNorm code sets (medications and medication allergens), integration of external sources such as coding systems for diagnosis or peri-operative systems. Optional implementation services are available.
§ 170.315(c)(2) CQM - Import and Calculate	CQM - Import and calculate supports thePromoting Interoperability definition and IPPS/ IQR program requirement for CEHRT for eCQMs. Includes the capability for an authorized user to import QRDA Category I and III data files and perform Clinical Quality Measure (CQM) calculations for the data for the measures to which the product is certified. **Relied upon software**: Health Services Analytics	This is included in the Soarian Clinicals certified modules utilizing the Health Services Analytics component. A software license for Soarian Clinicals is required. A software license to the Health Services Analytics components is required. CMS may change eCQM definitions and submission requirements from time to time and those changes may require software, configuration, and/or process updates which may incur optional or required costs.	Health Services Analytics has brand names including SQRS or Healthcare Intelligence including Clinical Intelligence and Quality Measures Intelligence, or DSS and SQM and Healthcare Query. If clients are using 3rd party vendor data warehouse products for eMeasure calculation, they are not relying on our certified capability but relying on third party capabilities to meet the 170.315(c)(1) - (3) criteria, and are likely using custom extracts required by that third--party data warehouse for exporting data from the source clinical EHR by a non-certified capability. To enable the certified capability to be used, configuration should be considered such as; configuration of reference build to map clinical data to the standard value sets, additional reference data build to support EH reporting, FDB Interoperability Module licensing for RxNorm code sets, integration of external sources such as coding systems for diagnosis or peri-operative systems. Optional implementation services are available.
§ 170.315(c)(3) CQM – Report	CQM - Report Promoting Interopability definition and IPPS/ IQR program requirement for CEHRT for eCQMs. **Relied upon software**: Health Services Analytics	This is included in the Soarian Clinicals certified modules utilizing the Health Services Analytics component. A software license for Soarian Clinicals is required. A software license to the Health Services Analytics components is required. A service is required for electronic submission of quality data. CMS may change eCQM definitions and submission requirements from time to time and those changes may require software, configuration, and/or process updates which may incur optional or required costs.	Health Services Analytics has brand names including SQRS or Healthcare Intelligence including Clinical Intelligence and Quality Measures Intelligence, or DSS and SQM and Healthcare Query. If clients are using 3rd party vendor data warehouse products for e-submission, they are not relying on our certified capability but relying on third party capabilities to meet the 170.315(c)(1) - (3) criteria, and are likely using custom extracts required by that third-party data warehouse for exporting data from the source clinical EHR by a non-certified capability. To enable the certified capability to be used, configuration should be considered such as; configuration of reference build to map clinical data to the standard value sets, additional reference data build to support EH and EP reporting, FDB Interoperability Module licensing for RxNorm code sets, integration of external sources such as coding systems for diagnosis or peri-operative systems.
§ 170.315(d)(1) Authentication, Access Control, and Authorization	Authentication, Access Control & Authorization applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports unique user identification, enables authentication against unique user identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module. Note that the API capability of the Soarian Clinicals modules (reference 170.315(g)(7) - (g)(9)) utilizes the oAuth2 and SAML services, per the technical specifications, for authentication, access control and authorization. In practice, utilization of these API services relies on a single, external, patient-facing identity provider (IdP) compatible with the API technical	To enable the certified capability to be used, configuration of the certified module for user accounts, security privileges, authentication parameters and related access controls per product documentation is presumed to be in place for any implementation. As to the intended use of certified capability, it is assumed that part of standard implementation requires definition and administration of users, security roles, authorization and authentication parameters and the like. Use of any advanced authentication methodologies such as biometrics or cryptographic methods used in two factor authentications are beyond the scope of certified product capabilities, but Cerner does support their use within the scope of product documentation. Similarly, use of any external authentication methods, such as SAML that are pass-through to the certified product's security services are beyond the scope of the certified capabilities but are not incompatible with

	control the specific access and privilege rights a user is granted. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	specifications for consumer user's authentication and access control. The IdP may be federated for use by more than one connected application or may be provided as embedded in a single connected application. Additional costs may apply for the IdP.	their use. Use of any external directory services, such as Client Directory Support, for user account or credential management also is beyond the scope of Cerner's certified capabilities but is not incompatible with their use.
§ 170.315(d)(2) Auditable Events and Tamper Resistance	Auditable Events and Tamper Resistance applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports event creation capabilities for security auditing of access to and actions on ePHI via the certified application, including integrity protection of recorded audit logs. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Establishing appropriate system clocks to standard time servers is part of initial system implementation and operations per product documentation. To enable the certified capability to be used, configuration of desired audit events for logging have been identified and implemented as part of standard implementation.
§ 170.315(d)(3) Audit Reports	Audit Reports applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	To enable the certified capability to be used standard reporting capabilities are included. Establishing appropriate system clocks to standard time servers is part of initial system implementation and operations per product documentation. Client review and maintenance of audit records is outside the scope of certification criteria.
§ 170.315(d)(4) Amendments	Amendments applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables recording of an amendment to a patient record based on a patient request, as well as the patient requests for amendment to their health record, including identification of whether the amendment was approved or denied.	Implementation of this capability is optional by clients and possessory rights to Soarian DM exist for Soarian clients. Implementation requires Soarian Document Management licensing.	As to the intended use of certified capability it is assumed that client definition and use of amendment capabilities should be flexible based on their form and manner of recording patient requested amendments. Amendments of ePHI maintained in non-certified systems or third-party systems certified for this criterion is beyond the scope of Cerner's certified capability but Cerner recognizes they may be in use for maintenance of ePHI beyond the scope of records maintained by our certified system. To enable the certified capability to be used, documentation templates can be defined both for recording patient requests/provider response and for the substance of the amendment request content. Accepting the amendment request into the record may involve use of additional documentation tools to create and persist medical record entries out of amendment requests such as for documenting patient contributed health information depending on its form.

	This criterion is conditionally required for certain certified modules and is provided by the *Soarian DM* certified module. It is also included in the Soarian Clinicals certified module using Soarian DM as required associated software. **Relied upon software**: Soarian Document Management		
§ 170.315(d)(5) Automatic Log-Off	Automatic Log-Off applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables automatic termination of a user session after a specified period of inactivity requiring re-authentication. This criterion is conditionally required for certain certified modules and is included in the Soarian Clinicals, Patient Portal – MMD, Provider Portal and Soarian DM certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	As to the intended use of certified capability it is assumed that Configuration will support both session suspension and termination after an interval of time. Configuration of automatic log off may be dependent on capabilities of the end user access point if beyond scope of what end user devices are normally presumed to be in use. To enable the certified capability to be used configuration is performed during standard implementation.
§ 170.315(d)(6) Emergency Access	Emergency Access applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables a limited set of specified users to access electronic health information in emergency scenarios. This criterion is conditionally required for certain certified modules and is included in the Soarian Clinicals and Soarian DM certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Use of business continuity and disaster recovery techniques and tools are beyond the scope of the intent of emergency access capabilities within the certified product as tested by certification testing but are relevant for HIPAA Security compliance and overall security risk assessment processes. To enable the certified capability to be used configuration of user positions with privilege to invoke the emergency access relationship type need to be defined as well as any desired logging of reasons for access. As to the intended use of certified capability it is assumed that the capability allows for override of restrictions on a user's ability to access records beyond the organization they are associated to, of encounter records marked as subject to confidentiality levels and based upon the access rights that may be defined for the emergency mode of access relationship type.
§ 170.315(d)(7) End-User Device Encryption	End User Device Encryption applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. The certified product is designed to prevent any persistent storage of electronic health information accessed in the *Soarian Clinicals* application locally to end-user devices (e.g. temp files, cookies, caches). This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules.	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	As to the intended use of certified capability it is assumed that End user device storage is not otherwise utilized for other applications within scope of Cerner's certified products. Cerner recommends end user device encryption beyond the certified capability for additional risk mitigation because of additional capabilities such as other applications and/or commercial copy/paste capabilities. Use of other encryption capabilities such as external end user disk encryption or encryption of enterprise/back end storage systems is beyond the scope of certification testing and the scope of certified modules.

	Relied upon software: N/A		
§ 170.315(d)(8) Integrity	Integrity applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables verification that health information exchanged electronically (both outbound and inbound) has not been altered during transmit via use of message digests produced by hash algorithms of SHA-2 or greater strength. This criterion is conditionally required for certain certified modules and is included in the Soarian Clinicals certified modules including AIS for integrity as it applies to secure transport for 170.315(b)(1) and data export 170.315(b)(6) and ePrescribing for integrity as it applies to 170.315(b)(3). **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Cerner OPENLink may be optionally configured for integrity of interface transactions but is outside the scope of certification criteria. To enable the certified capability to be used, integrity protection is enabled principally for secure transport of clinical information between entities / components based on protocols, certificates, ciphersuites and other network security protections such as public/private network security.
§ 170.315(d)(9) Trusted Connections	Trusted connections apply to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables the secure encryption and integrity-protection of electronic health information transmitted to external applications via API for patient access, and contribution of data from external applications for patient health information capture. This criterion is conditionally required for certain certified modules and is included in the Soarian Clinicals, Soarian DM, Patient Portal – MMD, and Provider Portal certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Product implemented trusted connections are enabled principally for secure transport of clinical information between entities / components based on protocols, certificates, ciphersuites and other network security protections such as public/private network security.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. **Relied upon software:** N/A	N/A	N/A

170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. **Relied upon software:** N/A	N/A	N/A
§ 170.315(f)(1) Transmission to Immunization registries	Transmission to Immunization applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability objective for active engagement in public health. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A Soarian Clinicals Software License is required including implementation of Med Administration Check.	Agency documentation of the appropriate state of active engagement is required and outside the scope of certified capability. Autoprofile web service is required to include immunization information in the summary of care. Bi-directional query capability requires integration with the registry.
§ 170.315(f)(2) Transmission to Public Health Agencies – Syndromic Surveillance	Transmission to Public Health Agencies – Syndromic Surveillance applies to the ONC 2015 Edition certification criterion utilized by a variety of federal & state programs including the Promoting Interoperability objective for active engagement in public health. **Relied upon software**: Cerner OPENLink	This is included with the Soarian Clinicals certified modules. A license is required for the Soarian Clinicals. Cerner OPENLink and model maps are required for connection to agency(ies).	Agency documentation of the appropriate state of active engagement is required and outside the scope of certified capability. To enable the capability, implementation of the syndromic interface is required in order to route the appropriate transactions.
§ 170.315(f)(5) Transmission to Public Health Agencies — Electronic Case Reporting	Enables automated creation of electronic case reports for public health reporting based on reportable condition triggers. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A license is required for the Soarian Clinicals. Cerner OPENLink and model maps are required for connection to agency(ies).	Agency documentation of the appropriate state of active engagement is required and outside the scope of certified capability. To enable the capability, implementation of 'trigger problems' must be defined in the workflow engine, also an SOEN document should be defined that supports USCDI v1.
§ 170.315(f)(6) Transmission to public health agencies — antimicrobial use and resistance reporting	Transmission to Public Health Agencies – Antimicrobial use and Resistance reporting applies to the ONC 2015 Edition certification criterion utilized to report the antimicrobial use and resistance data to the CDC's National Healthcare Safety Network (NHSN) for tracking and trend analysis. **Relied upon software**: N/A	This is included with the Soarian Clinicals certified modules. A license is required for Soarian Clinicals which includes the Pharmacy and Medication Administration Check modules. A Laboratory Information System is required that can transmit (using minimum HL7 2.5.1 version) the required NHSN information (organism and antimicrobial result) to the Pharmacy module.	An NHSN client account is required. The certified reporting capabilities require up-front configuration to define antimicrobials and susceptibility results, and National Healthcare Safety Network (NHSN) location mapping. Dependent on the LIS, additional up-front configuration might be required as well. Up front configuration includes interface mapping between the LIS and Pharmacy and NHSN
§ 170.315(g)(2) Automated Measure Recording	Enables calculation of numerator and denominator values as necessary for the Promoting Interoperability objectives. **Relied upon software**: N/A	Measure recording is included in the Soarian Clinicals certified modules for documented measures utilizing the Health Services Analytics component. A software license for Soarian Clinicals is required. A software license to the Health Services Analytics components is required.	Health Services Analytics has brand names including SQRS or Healthcare Intelligence including Clinical Intelligence and Quality Measures Intelligence, or DSS and SQM and Healthcare Query. To enable the certified capability reports must be configured to operational processes and data for measure requirements such as denominator qualification and reporting entities. As to the intended use of certified capability it is assumed that the standard reports are designed to work with particular certified product capabilities and workflows. Information on the design assumptions of the reports is available in Cerner reference documentation. Use of self-developed components or use of workflows that are beyond the scope of the design assumptions of the standard reporting may not result in measurement consideration. Use of self-developed reporting or process to compile numerator and denominator data from different sources than the certified

			modules may be possible with optional integration but are outside the scope of certified capabilities. Clients who have optionally licensed for Patient Portal – MMD, can utilize a report (accessible from the MMD solution) to generate both the numerator and denominator for the Patient Electronic Access objective. Clients who have not licensed for the Patient Portal – MMD solution, are required to rely on the Identity Provider for the numerator and a report from Soarian Clinicals for the denominator.
§ 170.315(g)(3) Safety Enhanced Design	Defines user-centered design processes and assessments for applicable certified capabilities within the certified product's scope. **Relied upon software**: N/A	Safety Enhanced Design is included with the Soarian Clinicals certified modules. No separate licensing is required.	N/A
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	Quality Management System applies to all certified modules listed herein. No separate licensing is required.	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	Accessibility Centered Design applies to all certified modules listed herein. No separate licensing is required.	N/A
§ 170.315(g)(6) CCDA Creation performance	CCDA creation performance applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives for patient engagement and coordination of care among providers. Enables the creation of a standards-conformant Consolidated Clinical Document Architecture (C-CDA) document, including Common Clinical Data Set (CCDS) representation. **Relied upon software**: N/A	A license for Soarian Clinicals is required. Clients are expected to stay current on software and codes / content for the data that comprises the C-CDA. Clients are expected to implement the processes and capabilities that cover the capture of the CCDS in care processes and the manual or automatic generation of the C-CDA with Clinical Letter capabilities. Advisory and implementation services are optional and recommended.	The C-CDA creation performance capabilities are supported as per ONC policy with certification of 170.315(b)(1), 170.315(b)(2), 170.315(b)(4), and 170.315(b)(6) criteria for creation of a C-CDA documents. Appropriate implementation and maintenance of medical code sets for vocabulary constraints and mapping of demographics data elements to defined standards is a pre-requisite for conformant C-CDA generation. Use of any non-certified capability for the recording of required structured clinical data to be included in C-CDA documents may not be compatible with certified capabilities. This criterion is essentially the subset of transitions of care criterion (reference 170.315(b)(1)) related to the capture of the CCDS and generation of a consolidated clinical document architecture (C-CDA) document.
§ 170.315(g)(7) Application access – Patient selection	Application access – patient selection applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives for patient engagement. This criterion includes an application programming interface (API) and is used in tandem with criteria for application access to patient health data (reference 170.315(g)(8) and (g)(9)) by patients and their authorized representatives using an Application configured to the technical and terms of use specifications of the certified API. Includes the capability to uniquely match and authenticate a request for access to health information from an external application of the patient's choice via the *Ignite Soarian API* to the correct Soarian patient record. **Relied upon software**: Ignite Soarian API	This is included in the Soarian Clinicals certified modules. A license for Soarian Clinicals is required. A one-time set-up for the Ignite Soarian API is required. An Application connection service is required for each application registered for use with the certified capability. API utilization subscription services may apply. Advisory and implementation services are optional and recommended.	As noted for criteria 170.315(d)(1), the API includes services for authentication, access control, and authorization; to utilize these services, a single, federated or application-provided, consumer-facing identity provider (IdP) that meets the technical specifications is required for all connected Applications. One or more Applications validated by Cerner to meet the Technical and Terms of Use specifications is required to utilize the certified capability. The Application(s) used must be used for Patient Access only. Providers must approve, register and implement the Application(s) for use in their environment. Application capability is outside the scope of the certified capability and may incur additional cost.

§ 170.315(g)(9) Application access – All data request	Application access – all data request applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including objectives for patient engagement. This criterion includes an application programming interface (API) and is used in tandem with criteria for application access to patient health data (reference 170.315(g)(7) and (g)(8)) by patients and their authorized representatives using an Application configured to the technical and terms of use specifications of the certified API. Includes the capability to respond to authenticated requests for health information via *the Ignite Soarian API* with the full Common Clinical Data Set (CCDS) using the C-CDA Continuity of Care Document (CCD) template, including accommodation of specific dates/date ranges. **Relied upon software**: Ignite Soarian API	This is included in the Soarian Clinicals certified modules. A license for Soarian Clinicals is required including AIS Archive. A one-time set-up for the Ignite Soarian API is required. As noted for criteria 170.315(d)(1), the API includes services for authentication, access control, and authorization; to utilize these services, a single, federated or application-provided, consumer-facing identity provider (IdP) that meets the technical specifications is required for all connected Applications. One or more Applications validated by Cerner to meet the Technical and Terms of Use specifications is required to utilize the certified capability. The Application(s) used must be used for Patient Access only. Providers must approve and implement the Application(s) for use in their environment. Application capability is outside the scope of the certified capability and may incur additional cost. Application connection service is required for each application registered for use with the certified capability. API utilization subscription services may apply. Advisory and implementation services are optional and recommended.	Clients are expected to stay current on software and codes / content for the data that comprises the CCDS / C-CDA. Clients are expected to implement the processes and capabilities that cover the capture of the CCDS in care processes and the manual or automatic generation of the C-CDA with Clinical Letter capabilities.
§ 170.315(g)(10) Standardized API for patient and population services	Standardized API – applies to the ONC 2015 Cures Edition certification criteria and replaces the § 170.315(g)(8) Application access – data category request criteria. This criterion includes an application programming interface (API) and is used in tandem with criteria for application access to patient health data (Reference 170.315(g)(7) and (g)(8) by patients and their authorized representatives and provides standardized access to single patient and multiple patient services via an API using the HL7 FHIR standard. Providers are granted independence when selecting third party services to use to interact with the acquired API technology. Patients gain the ability to securely access their health information using the application of their choice at no cost. **Relied upon software**: Ignite Soarian API and Apigee Edge	This is included in the Soarian Clinicals certified modules. A license for Soarian Clinicals is required. A one-time set-up for the Ignite Soarian API is required (fees can be found here; Certified Health IT | Cerner). Application capability is outside the scope of the certified capability and may incur additional cost. Application connection service is required for each application registered for use with the certified capability. API utilization subscription services may apply. Clients are expected to stay current on software and codes / content for the data that comprises the CCDS/USCDI. Clients are expected to implement the processes and capabilities that cover the capture of the CCDS/USCDI in care processes. There are required and optional advisory and implementation services available.	As noted for criteria 170.315(d)(1), the API includes services for authentication, access control, and authorization; to utilize these services, a single, federated or application-provided, consumer-facing identity provider (IdP) that meets the technical specifications is required for any and all connected Applications. One or more Applications validated by Cerner to meet the Technical and Terms of Use specifications is required to utilize the certified capability. Additional implementation and authorization information can be found and referenced here; https://fhir.cerner.com/soarian/overview/
§ 170.315(h)(1) Direct Project	Includes the capability to exchange health information with external entities using the Direct Project standards for Secure Health Transport. **Relied upon software**: *Cerner Direct Messaging*	This is included in the Soarian Clinicals certified module that is inclusive of Cerner Direct Messaging HISP for this criterion. A license for Soarian Clinicals is required including AIS (also referred to as HUB-HIE). To implement and use this possessed capability, a license for Cerner Direct Messaging HISP including integration with the AIS via the Direct XDR for Cerner Direct Messaging HISP service is required.	Use of Cerner Direct Messaging HISP requires that clients complete a current Cerner Direct Messaging certificate request containing required Trust Framework contents that establish and validate Clients' authenticity and parameters under which client may participate in Direct exchange. Use of the certified capability depends on known trusted users who have Direct accounts and the use of transacting with non-Direct users is outside of the scope of use for the certified product. Implementation and use of this capability by providers for transitions of care or secure messaging is optional; possession as part of Base CEHRT definition is required.

Soarian DM (Soarian Document Management) *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. Organizations may incur ancillary costs for use of the patient population export for encrypted device(s), local network and/or (ultimately) cloud storage of the exported data.	Implementation and use of the single patient EHI Export capability involves as a pre-requisite step of an upgrade to 25.4 SP6 U4 Soarian Document Management code level. Implementation and use of the patient population export capability involves a set of pre-requisites, including a software upgrade to SDM 25.4 SP6 U4. A signed PECA must be provided along with ensuring system connectivity. For Remote Hosted customers, suitable Apricorn Drives to store 2x DM storage will need to be provided. For Client Hosted customers the following will need to be provided: • The UNC/Drive extraction path that is 2x DM storage • Procure server to run extract from with the following: System Type: x64-based PC; OS: Windows Server, Physical Mem: 12 GB, Virtual Mem: 8 GB, Page File: 4 GB, HD Space: 500 GB • Install Notepad++ and Acrobat Reader on extraction device • Extraction directories must be excluded from virus scanning software. • Notify Direct Line/Custom Services to start extraction and include the Apricorn drives (Remote Hosted) or UNC extract location (Client Hosted). Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(d)(1) Authentication, Access Control, and Authorization	Authentication, Access Control & Authorization applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports unique user identification, enables authentication against unique user identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. This criterion is conditionally required for all certified modules and is included in the Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Use of any advanced authentication methodologies such as biometrics or cryptographic methods used in two factor authentications are beyond the scope of certified product capabilities, but Cerner does support their use within the scope of product documentation. Similarly, use of any external authentication methods, such as SAML that are pass-through to the certified product's security services are beyond the scope of the certified capabilities but are not incompatible with their use. Use of any external directory services, such as Client Directory Support, for user account or credential management also is beyond the scope of Cerner's certified capabilities but is not incompatible with their use.

§ 170.315(d)(2) Auditable Events and Tamper Resistance	Auditable Events and Tamper Resistance applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports event creation capabilities for security auditing of access to and actions on ePHI via the certified application, including integrity protection of recorded audit logs. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	To enable the certified capability to be used, configuration of desired audit events for logging have been identified and implemented as part of standard implementation.
§ 170.315(d)(3) Audit Reports	Audit Reports applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Establishing appropriate system clocks to standard time servers is part of initial system implementation and operations per product documentation. Client review and maintenance of audit records is outside the scope of certification criteria.
§ 170.315(d)(4) Amendments	Amendments applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables recording of an amendment to a patient record based on a patient request, as well as the patient requests for amendment to their health record, including identification of whether the amendment was approved or denied. This criterion is conditionally required for certain certified modules and is provided by the *Soarian DM* certified module. It is also included in the Soarian Clinicals certified module using Soarian DM as required associated software. **Relied upon software**: Soarian Clinicals	Implementation of this capability is optional by clients and possessory rights to Soarian DM exist for Soarian clients. Implementation requires Soarian Document Management licensing.	To enable the certified capability to be used, documentation templates can be defined both for recording patient requests/provider response and for the substance of the amendment request content. Accepting the amendment request into the record may involve use of additional documentation tools to create and persist medical record entries out of amendment requests such as for documenting patient contributed health information depending on its form.
§ 170.315(d)(5) Automatic Log-Off	Automatic Log-Off applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for	To enable the certified capability to be used configuration is performed during standard implementation.

	Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables automatic termination of a user session after a specified period of inactivity requiring re-authentication. This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	the certified capability apart from the licensing required for the Health IT module.	
§ 170.315(d)(9) Trusted Connections	Trusted connections apply to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables the secure encryption and integrity-protection of electronic health information transmitted to external applications via API for patient access, and contribution of data from external applications for patient health information capture. This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, Soarian DM, Patient Portal – MMD, and Provider Portal* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Product implemented trusted connections are enabled principally for secure transport of clinical information between entities / components based on protocols, certificates, ciphersuites and other network security protections such as public/private network security.
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. **Relied upon software:** N/A	N/A	N/A
§ 170.315(e)(3) Patient Health Information Capture	Patient health information capture applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability objective for patient	This is included with the Soarian DM certified module. A Software license is required for the certified module (Soarian DM); no additional license is required for this	As to the intended use of certified capability clients need to utilize the capabilities defined in product documentation for appropriate attribution.

	engagement to allow patients and external providers to contribute to the patient record. Includes the capability for patients or their authorized representatives to securely and electronically provide health information from non-clinical settings to providers and care team members for incorporation into their health record. **Relied upon software**: N/A	capability. Optional advisory and implementation services are available.	
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	Quality Management System applies to all certified modules listed herein. No separate licensing is required.	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	Accessibility Centered Design applies to all certified modules listed herein. No separate licensing is required.	N/A

Patient Portal - MMD *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities. However, organizations may incur ancillary costs for use of the patient population export for an encrypted device for the exported data.	Implementation and use of the single patient EHI Export capability involves the pre-requisite of operating at a minimum v8.1 Patient Portal – MMD. The patient population export requires an encrypted device provided by the customer to load the export on, Due to the data volume and overall complexity of the operations, patient population EHI Export is executed by Provider Portal resources. Clients can initiate an export request by logging a service record (SR) in eService to the solution of Provider Portal. Please note that filtering the export by specific locations or other subsets within a Patient Portal - MMD system is not supported, nor is combining EHI across disparate Patient Portal - MMD systems. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
170.315(d)(1) Authentication, Access Control, and Authorization	Enables calculation of numerator and denominator values as necessary for the Promoting Interoperability objectives. **Relied upon software**: N/A	Automated Measure Recording is included with the Patient Portal - MMD, and Provider Portal certified modules to support measure reporting for (View download and transmit) VDT and/or secure messaging. A software license is required for the certified modules; no additional license is required for the reporting capabilities.	Use of any advanced authentication methodologies such as biometrics or cryptographic methods used in two factor authentications are beyond the scope of certified product capabilities but Cerner does support their use within the scope of product documentation. Similarly, use of any external authentication methods, such as SAML that are pass-through to the certified product's security services are beyond the scope of the certified capabilities but are not incompatible with their use. Use of any external directory services, such as Client Directory Support, for user account or credential management also is beyond the scope of Cerner's certified capabilities but is not incompatible with their use.
§ 170.315(d)(2) Auditable Events and Tamper Resistance	Auditable Events and Tamper Resistance applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports event creation capabilities for security auditing of access to and actions on ePHI via the certified application, including integrity protection of recorded audit logs. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	To enable the certified capability to be used, configuration of desired audit events for logging have been identified and implemented as part of standard implementation.
§ 170.315(d)(3) Audit Reports	Audit Reports applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Establishing appropriate system clocks to standard time servers is part of initial system implementation and operations per product documentation. Client review and maintenance of audit records is outside the scope of certification criteria.

	Security Risk Assessment and Implementation Plan. Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A		
§ 170.315(d)(5) Automatic Log-Off	Automatic Log-Off applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables automatic termination of a user session after a specified period of inactivity requiring re-authentication. This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	To enable the certified capability to be used configuration is performed during standard implementation.
§ 170.315(d)(7) End-User Device Encryption	End User Device Encryption applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. The certified product is designed to prevent any persistent storage of electronic health information accessed in the *Soarian Clinicals* application locally to end-user devices (e.g. temp files, cookies, caches). This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	
§ 170.315(d)(9) Trusted Connections	Trusted connections apply to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables the secure encryption and integrity-protection of electronic health information transmitted to external applications via API for patient access, and contribution of data from	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Product implemented trusted connections are enabled principally for secure transport of clinical information between entities / components based on protocols, certificates, ciphersuites and other network security protections such as public/private network security.

	external applications for patient health information capture. This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, Soarian DM, Patient Portal – MMD, and Provider Portal* certified modules. **Relied upon software**: N/A		
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases. **Relied upon software:** N/A	N/A	N/A
§ 170.315(e)(1) View, Download, and Transmit	View, Download and Transmit applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability objectives for patient engagement to provide patients and their authorized representatives the ability to view, download or transmit their health data. Includes the capability for patients and their authorized representatives to access their health information electronically, and download and transmit it to a 3rd party (via both secure encrypted and unencrypted methods) in a C-CDA format using the Continuity of Care Document (CCD) template. Also includes the ability to view health information associated with a specific date and/or date range and access a detailed activity history log of actions in their portal. **Relied upon software**: N/A	This is included with the Patient Portal – MMD certified module. A Software license for the patient portal is required. The Provider Portal license is optional for enabling transmit among patients and clinicians configured in the infrastructure. The Cerner Direct Messaging HISP service subscription is optional if secure transport to third party is enabled outside the patient and provider portal infrastructure. Optional costs are additional services for exchange that may be available by participation through other intermediaries. Implementation of patient consent is required and costs apply. To enable full measure reporting, an ADT interface is required for denominator evaluation. Integration of EMR(s) and/or HIE(s) as the source(s) for summaries of care is required and integration costs may apply.	To enable full measure reporting, an ADT interface is required for denominator evaluation. Integration of EMR(s) and/or HIE(s) as the source(s) for summaries of care is required and integration costs may apply. Summary of care documents need to be available to patients within measure reporting time limits for EH/EP; if ADT encounter information is available, portal reports may calculate time limits, otherwise will report availability for alternative report calculation. Patient provisioning or enabling of optional automated and/or self-provisioning features is required to ensure patient independent access to health care information.
§ 170.315(g)(2) Automated Measure Recording	Enables calculation of numerator and denominator values as necessary for the Promoting Interoperability objectives. Measure reporting for patient health information capture (reference 170.315(e)(3)) criterion in Soarian DM is performed with associated software in the Soarian Clinicals certified modules for Health Services Analytics.	Automated Measure Recording is included with the Patient Portal - MMD, and Provider Portal certified modules to support measure reporting for (View download and transmit) VDT and/or secure messaging. A software license is required for the certified modules; no additional license is required for the reporting capabilities.	As to the intended use of certified capability it is assumed that the standard reports are designed to work with particular certified product capabilities and workflows. Information on the design assumptions of the reports is available in Cerner reference documentation. Use of self-developed components or use of workflows that are beyond the scope of the design assumptions of the standard reporting may not result in measurement consideration. Use of self-developed reporting or process to compile numerator and denominator data from different sources than the certified

	Relied upon software: N/A		modules may be possible with optional integration and configuration but are outside the scope of Cerner's certified capabilities.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	Quality Management System applies to all certified modules listed herein. No separate licensing is required.	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	Accessibility Centered Design applies to all certified modules listed herein. No separate licensing is required.	N/A

NOVIUS Lab *See Appendix A for certified versions and CHPL listing information*

This Health IT Module is compliant with the ONC Certification Criteria for Health IT 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.

Certified Capability	Description of Capability & Additional Relied Upon Software	Types of Costs/Fees	Significant Implementation Guidance
§ 170.315(b)(10) Electronic Health Information (EHI) Export	Supports the ability to export all EHI stored in or by the certified HIT module, or the product of which it is a part, for a single patient and/or full patient population in an electronic and computable (machine-processable) format. **Relied upon software**: N/A	There are no required costs imposed by Cerner for use of the EHI Export capabilities.	The EHI Export capability requires NOVIUS Lab Version 27.2.5. Clients who want to perform the All Patient Export need to ensure they have a server or external drive with enough space to copy the exported data. Once the data has been exported, an eService Request to NOVIUS Lab support can be opened to configure Offline Archive Processing to export the archived patient reports. Data format specifications for both the single patient and patient population exports are publicly accessible at https://www.oracle.com/health/regulatory/certified-health-it/ (see under the "EHI Export" heading).
§ 170.315(d)(1) Authentication, Access Control, and Authorization	Authentication, Access Control & Authorization applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports unique user identification, enables authentication against unique user identifiers (i.e. username/password) to gain access to electronic health information, and includes the ability to control the specific access and privilege rights a user is granted. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Use of any advanced authentication methodologies such as biometrics or cryptographic methods used in two factor authentications are beyond the scope of certified product capabilities but Cerner does support their use within the scope of product documentation. Similarly, use of any external authentication methods, such as SAML that are pass-through to the certified product's security services are beyond the scope of the certified capabilities but are not incompatible with their use. Use of any external directory services, such as Client Directory Support, for user account or credential management also is beyond the scope of Cerner's certified capabilities but is not incompatible with their use.
§ 170.315(d)(2) Auditable Events and Tamper Resistance	Auditable Events and Tamper Resistance applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Supports event creation capabilities for security auditing of access to and actions on ePHI via the *FirstNet* application, including integrity protection of recorded audit logs. This criterion is conditionally required for all certified modules and is included in the Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM certified modules.	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	To enable the certified capability to be used, configuration of desired audit events for logging have been identified and implemented as part of standard implementation.

	Relied upon software: ntpd (Linux)		
§ 170.315(d)(3) Audit Reports	Audit Reports applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. Enables creation of sortable audit reports for specific time frames, and based on specific parameters such as user ID, patient ID, type of action, etc. This criterion is conditionally required for all certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	Establishing appropriate system clocks to standard time servers is part of initial system implementation and operations per product documentation. Client review and maintenance of audit records is outside the scope of certification criteria.
§ 170.315(d)(7) End-User Device Encryption	End User Device Encryption applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including thePromoting Interoperability Base CEHRT definition and supports the development and maintenance of a Privacy and Security Risk Assessment and Implementation Plan. The certified product is designed to prevent any persistent storage of electronic health information accessed in the *Soarian Clinicals* application locally to end-user devices (e.g. temp files, cookies, caches). This criterion is conditionally required for certain certified modules and is included in the *Soarian Clinicals, NOVIUS Lab, Patient Portal – MMD, Provider Portal and Soarian DM* certified modules. **Relied upon software**: N/A	No separate licensing for this capability is required. The capabilities are considered a core component of the Health IT module itself, and no separate licensing is required for the certified capability apart from the licensing required for the Health IT module.	N/A
170.315(d)(12) Encrypt Authentication Credentials	Identifies whether the certified product enables FIPS 140-2 compliant encryption or cryptographic hashing of end-user credentials stored within the product. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. **Relied upon software:** N/A	N/A	N/A
170.315(d)(13) Multi-Factor Authentication	Identifies whether the certified product enables multi-factor authentication (MFA) in accordance with industry-recognized standards. This criterion is intended exclusively for market transparency purposes and there is no requirement to implement or use any relevant capabilities. See Cerner.com/certified-health-it for details on any supported MFA use-cases.	N/A	N/A

	Relied upon software: N/A		
§ 170.315(f)(3) Transmission to Public Health Agencies – Reportable Laboratory Tests and Values/Results	Transmission of Reportable Lab Results applies to the ONC 2015 Edition certification criterion utilized by a variety of federal and state programs including the Promoting Interoperability objective for active engagement in public health. Enables creation and transmission of laboratory tests and results data to external public health agencies formatted according to the HL7 2.5.1 standards for Electronic Laboratory Reporting to Public Health. **Relied upon software**: N/A	This capability is included with the NOVIUS Lab certified module. A license is required for NOVIUS Lab; no additional license is required for this capability. Cerner OPENLink is optionally utilized for connection to agency(ies) and interface customization.	To enable the capability, master files need to be updated for required codes and interfaces configured.
§ 170.315(g)(4) Quality Management System	Establishes controls for and monitors compliance with the quality standards under which the included certified capabilities are developed, tested, implemented, and maintained. **Relied upon software**: N/A	Quality Management System applies to all certified modules listed herein. No separate licensing is required.	N/A
§ 170.315(g)(5) Accessibility Centered Design	Encompasses the processes by which the accessibility standards employed in the development of the certified capabilities. **Relied upon software**: N/A	Accessibility Centered Design applies to all certified modules listed herein. No separate licensing is required.	N/A

Appendix A: Active Certified Health IT Module Versions

Antimicrobial Usage and Resistance Reporting		
Version	**CHPL Product Number**	**Date Certified**
2	15.04.04.1221.Anti.02.08.1.240319	March 19, 2024

Electronic Case Reporting		
Version	**CHPL Product Number**	**Date Certified**
1	15.04.04.1221.Case.01.00.1.211229	December 29, 2021

Health Data Intelligence: eCQMs		
Version	**CHPL Product Number**	**Date Certified**
2024	15.04.04.1221.Heal.24.00.0.241224	December 24, 2024

HealtheAnalytics: Promoting Interoperability		
Version	**CHPL Product Number**	**Date Certified**
2024	15.04.04.1221.HAna.24.05.0.240319	March 19, 2024

HealthSentry		
Version	**CHPL Product Number**	**Date Certified**
2023	15.04.04.1221.Heal.23.06.1.230331	March 31, 2023

Millennium (Clinical)		
Version	**CHPL Product Number**	**Date Certified**
*2018	15.04.04.1221.Mill.18.06.1.221107	November 7, 2022
2024	15.04.04.1221.Mill.24.07.1.240920	September 20, 2024

***Requires minimum minor sub-release of 2018.08 or higher**

Millennium (CQMs)		
Version	**CHPL Product Number**	**Date Certified**
2018	15.04.04.1221.Mill.18.04.1.220101	January 1, 2022
2024	15.04.04.1221.Mill.24.05.1.240814	August 14, 2024

Millennium (Health Care Surveys)		
Version	**CHPL Product Number**	**Date Certified**
2018	15.04.04.1221.Mill.HC.03.1.220101	January 1, 2022
2024	15.04.04.1221.Mill.HC.04.0.241009	October 9, 2024

Millennium (Immunizations)		
Version	**CHPL Product Number**	**Date Certified**
2018	15.04.04.1221.Mill.I8.03.1.220101	January 1, 2022
2024	15.04.04.1221.Mill.I4.04.1.241009	October 9, 2024

Patient Portal		
Version	**CHPL Product Number**	**Date Certified**
2024	15.04.04.1221.Pati.23.07.1.240101	January 1, 2024
1	15.04.04.1221.Pati.01.08.1.240801	August 1, 2024

PowerChart Touch		
Version	**CHPL Product Number**	**Date Certified**
4	15.04.04.1221.Powe.03.02.1.210308	March 8, 2021

Privacy Analytics		
Version	**CHPL Product Number**	**Date Certified**
5.0.4.1	15.04.04.1221.Priv.P2.01.1.180625	June 25, 2018
6	15.04.04.1221.Priv.06.01.1.180727	July 27, 2018
2024	15.04.04.1221.Priv.24.08.1.240101	January 1, 2024

Syndromic Surveillance and eLab Results		
Version	**CHPL Product Number**	**Date Certified**
1	15.04.04.1221.SyeL.01.00.0.240101	January 1, 2024

Soarian Clinicals		
Version	**CHPL Product Number**	**Date Certified**
2015	15.04.04.1221.Soar.15.01.1.210331	March 31, 2021

Soarian DM (Soarian Document Management)		
Version	**CHPL Product Number**	**Date Certified**
*2015	15.07.04.1221.Soar.DO.01.1.180720	July 20, 2018

***Requires minimum solution release of 25.02.02 or higher**

Patient Portal – MMD		
Version	**CHPL Product Number**	**Date Certified**
*2015	15.07.04.1221.Pati.MM.01.0.180720	July 20, 2018

***Requires minimum solution release of 4.5 or higher**

NOVIUS Lab		
Version	**CHPL Product Number**	**Date Certified**
*2015	15.07.04.1221.NOVI.NO.01.0.180720	July 20, 2018

***Requires minimum solution release of 27.2.1 or higher**

Appendix B: Certified Clinical Quality Measures (CQMs)

Note – all identified CQMs are certified for the criteria at 170.315(c)(1)-(3)

Certified HIT Module	Certified Clinical Quality Measures (CQMs)
Health Data Intelligence: eCQMs	• CMS2: Preventive Care and Screening: Screening for Depression and Follow-Up Plan • CMS122: Diabetes: Hemoglobin A1c (HbA1c) Poor Control (> 9%) • CMS165: Controlling High Blood Pressure
Millennium (CQMs)	• CMS2: Preventive Care and Screening: Screening for Depression and Follow-Up Plan • CMS9: Exclusive Breast Milk Feeding • CMS22: Preventive Care and Screening: Screening for High Blood Pressure and Follow-Up Documented • CMS50: Closing the Referral Loop: Receipt of Specialist Report • CMS56: Functional Status Assessment for Total Hip Replacement • CMS68: Documentation of Current Medications in the Medical Record • CMS69: Preventive Care and Screening: Body Mass Index (BMI) Screening and Follow-Up Plan • CMS71: Anticoagulation Therapy for Atrial Fibrillation/Flutter • CMS72: Antithrombotic Therapy By End of Hospital Day 2 • CMS74: Primary Caries Prevention Intervention as Offered by Primary Care Providers, including Dentists • CMS75: Children Who Have Dental Decay or Cavities • CMS90: Functional Status Assessments for Congestive Heart Failure • CMS104: Discharged on Antithrombotic Therapy • CMS105: Discharged on Statin Medication • CMS108: Venous Thromboembolism Prophylaxis • CMS111: Median Admit Decision Time to ED Departure Time for Admitted Patients • CMS113: Elective Delivery • CMS117: Childhood Immunization Status • CMS122: Diabetes: Hemoglobin A1c (HbA1c) Poor Control (> 9%) • CMS124: Cervical Cancer Screening • CMS125: Breast Cancer Screening • CMS127: Pneumococcal Vaccination Status for Older Adults • CMS130: Colorectal Cancer Screening • CMS131: Diabetes: Eye Exam • CMS135: Heart Failure (HF): Angiotensin-Converting Enzyme (ACE) Inhibitor or Angiotensin Receptor Blocker (ARB) Therapy for Left Ventricular Systolic Dysfunction (LVSD) • CMS137: Initiation and Engagement of Alcohol and Other Drug Dependence Treatment • CMS138: Preventive Care and Screening: Tobacco Use: Screening and Cessation Intervention • CMS139: Falls: Screening for Future Fall Risk • CMS144: Heart Failure (HF): Beta-Blocker Therapy for Left Ventricular Systolic Dysfunction (LVSD) • CMS145: Coronary Artery Disease (CAD): Beta-Blocker Therapy-Prior Myocardial Infarction (MI) or Left Ventricular Systolic Dysfunction (LVEF <40%)

	• CMS146: Appropriate Testing for Children with Pharyngitis • CMS147: Preventive Care and Screening: Influenza Immunization • CMS149: Dementia: Cognitive Assessment • CMS153: Chlamydia Screening for Women • CMS154: Appropriate Treatment for Children with Upper Respiratory Infection (URI) • CMS155: Weight Assessment and Counseling for Nutrition and Physical Activity for Children and Adolescents • CMS156: Use of High-Risk Medications in the Elderly • CMS157: Oncology: Medical and Radiation - Pain Intensity Quantified • CMS159: Depression Remission at Twelve Months • CMS161: Adult Major Depressive Disorder (MDD): Suicide Risk Assessment • CMS165: Controlling High Blood Pressure • CMS177: Child and Adolescent Major Depressive Disorder (MDD): Suicide Risk Assessment • CMS190: Intensive Care Unit Venous Thromboembolism Prophylaxis • CMS334: Cesarean Birth • CMS347: Statin Therapy for the Prevention and Treatment of Cardiovascular Disease • CMS349: HIV Screening • CMS 506: Safe Use of Opioids - Concurrent Prescribing • CMS816: Hospital Harm - Severe Hypoglycemia • CMS819: Hospital Harm - Opioid-Related Adverse Events • CMS871: Hospital Harm - Severe Hyperglycemia • CMS951: Kidney Health Evaluation • CMS986: Global Malnutrition Composite Score • CMS996: Appropriate Treatment for ST-Segment Elevation Myocardial Infarction (STEMI) Patients in the Emergency Department (ED) • CMS1028: Severe Obstetric Complications
Soarian Clinicals	• CMS9: Exclusive Breast Milk Feeding • CMS71: Anticoagulation Therapy for Atrial Fibrillation/Flutter • CMS72: Antithrombotic Therapy By End of Hospital Day 2 • CMS104: Discharged on Antithrombotic Therapy • CMS105: Discharged on Statin Medication • CMS108: Venous Thromboembolism Prophylaxis • CMS111: Median Admit Decision Time to ED Departure Time for Admitted Patients • CMS190: Intensive Care Unit Venous Thromboembolism Prophylaxis • CMS334: Cesarean Birth • CMS506: Safe Use of Opioids- Concurrent Prescribing • CMS816: Hospital Harm - Severe Hypoglycemia • CMS819: Hospital Harm - Opioid-Related Adverse Events • CMS871: Hospital Harm - Severe Hyperglycemia • CMS986: Global Malnutrition Composite Score • CMS1028: Severe Obstetric Complications