Part 11 in Title 21 Conformance Statement

This conformance statement has been updated for this release and is applicable to this and future releases unless updated: Clinical Release 6.0. Contact HealthMyne to ensure you have the most recent version of this statement.

Introduction

Part 11 in Title 21 of the Code of Federal Regulations includes the US Federal guidelines for storing and protecting electronic records and applying electronic signatures. The intent of these guidelines is to ensure that applicable electronic records are reliable, authentic and maintained with high integrity. HealthMyne QIDS only provides functionality to help you meet the technical requirements of Part 11 in Title 21 as it pertains to electronic records and signatures within the application. Organizational policies, your IT infrastructure, and other document controls play an important role in Part 11 in Title 21 compliance.

This document identifies where and how changes are recorded within HealthMyne QIDS that could be considered electronic records. It is intended for administrator and clinicians assessing their site's compliance to Part 11 in Title 21.

Part 11 in Title 21 categorizes systems as closed or open and it contains rules for systems that do and do not use biometrics as part of electronic signatures. When considering the regulations for your compliance:

- HealthMyne QIDS is a closed system since access is controlled by the clinic/clinic staff who are responsible for the content of electronic records that are on the system.
- HealthMyne QIDS only supports non-biometric electronic signatures.

Summary Checklist

The following checklist summarizes how HealthMyne QIDS meets the requirements of Part 11 in Title 21. See the additional sections for details on what is tracked within HealthMyne QIDS.

This checklist only considers those controls applicable to a closed system without biometric signatures and applies when the HealthMyne QIDS is installed and operated per HealthMyne recommended use and instructions.

Part 11 in Title 21	Brief Description	Compliance
11.10 (a)	Validation of systems	✓
11.10 (b)	Accurate & complete copies of records	✓
11.10 (c)	Protection of records	✓
11.10 (d)	Limiting access to authorized individuals	✓
11.10 (e)	Secure computer-generated time-stamped audit trails	✓
11.10 (f)	Use of operational system checks	✓
11.10 (g)	Use of authority checks	✓
11.10 (h)	Use of device checks	N/A
11.10 (i)	Suitable education, training & experience	Site standards of practice
11.10 (j)	Accountability & responsibility for electronic signatures	Site standards of practice
11.10 (k) (1)	Controls over distribution, use of and access to documentation	✓
11.10 (k) (2)	Audit trail of modifications to documentation	✓
11.50 (a) (1)	Signed electronic records include printed name of signer	✓
11.50 (a) (2)	Signed electronic records include time & date of execution	✓
11.50 (a) (3)	Signed electronic records include meaning of signature	✓
11.50 (b)	Subject to same controls as electronic records	✓
11.70	Electronic signatures linked to their records	✓
11.100 (a)	Signatures unique to one individual	✓
11.100 (b)	Organization to verify individual's identity	Site standards of practice
11.100 (c)	Declaration of equivalence to handwritten signature	Site standards of practice
11.200 (a) (1)	Use two distinct identification components	✓
11.200 (a) (1) (i)	Use at least one component on subsequent signings in same session	See the additional sections to determine compliance
11.200 (a) (1) (ii)	Use all components on signings in separate sessions	✓
11.200 (a) (2)	Used only by their genuine owner	✓
11.200 (a) (3)	Misuse requires collaboration of ≥2 individuals	✓
11.300 (a)	Identification code/password combination to be unique	✓
11.300 (b)	Periodically checked, recalled or revised	Site standards of practice
11.300 (c)	Loss management procedures for devices	Site standards of practice
11.300 (d)	Transaction safeguards to detect and prevent misuse	Site standards of practice
11.300 (e)	Periodic testing of devices	N/A

Secure Access

HealthMyne QIDS uses HTTPS for transferring data between clients and the servers within a local area network (LAN). We recommend you install your hardware (both clients and servers) behind a firewall to prevent unauthorized external access to the data and systems.

If you are allowing external access to the client software, we recommend using a secure channel such as a virtual private network (VPN). We recommend you install and maintain this product within a secure area of your clinic.

We recommend that you install and maintain anti-virus software on the client hardware.

We recommend you use an authentication and authorization tool for the hardware and operating system you use with this product to prevent unauthorized access. We do not allow users to log in without an authentication and authorization tool in place. We currently support LDAP authentication.

Users must log in using their user name and password. When launching from a 3rd party the LDAP authentication is used to validate that the user is authorized to enter HealthMyne QIDS.

Audit Log

The event browser displays actions performed in HealthMyne QIDS, who performed them, and the date and time. For example, opening a protocol or changing a report status, and logging in. The records of login and logout activities can help in identifying authorized and unauthorized access to HealthMyne QIDS.

Studies

Structures

Structures (for example, lesions and non-measured regions) are tagged with who created them and the date they were updated. Structures that are confirmed record the confirmation date.

Key Images

User created key images are tagged with who created them and the date/time they were created. Images are available as series in the study and contain the date they were created and the person who created them.

Metrics

Metrics exported to a CSV file and dictation do not include the date and person exporting the information. Dictation systems record the person and date performing the dictation, which includes the metrics from HealthMyne QIDS. We recommend you review your dictation system if necessary for compliance to Part 11 in Title 21.

Timeline

When custom events are added to the timeline, HealthMyne QIDS records the person editing the event and the most recent change date. That information is stored in the database but not displayed on-screen.

Incidental Findings

An incidental finding record is created or an existing record is updated with the date and the person identifying an incidental finding. Incidental findings records include a log of the date of a change and the person making the change: assigning a case coordinator, selecting a follow-up period, commenting, recording a phone contact, generation of a letter, and closing a case.

Cancer Screening

A cancer screening record is created with the date and the person identifying the patient as part of a cancer screening program. Cancer screening records include a log of the date of a change and the person making the change: assigning a case coordinator, selecting a follow-up period, commenting, recording a phone contact, generation of a letter, and closing a case. When studies arrive that match the screening record exam group, the system records that it added the study and the date (the user is recorded as the system).

Tumor Conference

When a tumor conference starts the information for the included patients are locked. The sections display the date of last update and the person who made the update. When a conference is finalized and closed the conference is locked and the persons attending, and the date and person finalizing the conference are recorded and displayed.

Reports

Lung-RADS, Therapy Response, Lung Density, Emphysema, and Heterogeneity

For reports that have worksheets (before a report is saved), the date and person are recorded in the database when the worksheet is created. If there are changes to the report (for example, a note is added, or a warning is resolved) the date and the person for the change are recorded and part of the report. Preliminary and final reports contain the date the report was created and the person who created it. Reports are set up to be printed or saved electronically, with the creation information.

QIMR and QTBR

For QIMR and QTBR when you export the report to DICOM it is available as a DICOM series in the study and contains the date it was created and the person who created it.