EpicCare®

21 CFR Part 11 Compliance And Epic

Last Revised: September 25, 2003

Epic Systems Corporation

1979 Milky Way • Verona, WI 53593 • Voice: (608) 271-9000 • Fax: (608) 271-7237

www.epicsystems.com

Important Notice Regarding Use of Epic Software

Epic Systems Corporation software is intended solely for use by competent healthcare professionals applying their medical skill, intellect and experience to make all judgments and decisions that affect patient health. Epic software and the data contained therein should not be used either as a substitute for the independent medical decisions of competent healthcare professionals or as the primary basis for monitoring or alerting health care professionals as to a patient's condition, course of treatment, diagnosis or prognosis. Epic software and the data contained therein should not be used in any manner that is not expressly described in the manuals provided by Epic with respect to the applicable software. All users of Epic software must implement tested and reliable processes for ensuring competent human decision-making in all actions impacting patient health or safety and must practice them at all times.

The information in this document is intended solely as a preliminary guide on the issues discussed herein. It is not intended to represent that the described Epic functionality is necessary or sufficient for compliance with 21 CFR Part 11 requirements. The design and implementation of specific system components requires the advice of a professional familiar with your individual situation. The information in this document can not take the place of that advice. If specific questions arise regarding the information discussed herein, contact a systems professional. Users of this document agree to hold Epic Systems Corporation harmless from any liability or damages arising from such use. Use of this document indicates your understanding of and agreement with these conditions and your ability to bind your company to these terms. If you do not understand or agree to these conditions or if you are not able to agree to these terms for your company, then do not use this document.

TABLE OF CONTENTS

ABSTRACT

This paper is intended for those concerned with the capability of Epic's software to assist in complying with Electronic Records and Electronic Signature specifications in Title 21 Code of Federal Regulations Part 11. Epic's quality assurance procedures, system controls, staff qualifications, and policies for documenting system changes are discussed.

Epic's system has features that can help an organization that submits electronic records to the FDA comply with 21 CFR Part 11 as described below. Organizations assessing their compliance should confirm that they have set Epic's system up and have established processes supporting it in a manner appropriate for the relevant regulation.

Electronic Records

Epic's system provides several controls to restrict record access and documentation functions to appropriate users, and to log information about contributions to the record.

System Validation

While you will perform the system validation testing you deem necessary for compliance, Epic has procedures in place to confirm that the system works as expected before releasing it to clients. Epic uses tracking logs to document and manage development of new system features and modifications to existing functions. We have an intensive quality assurance process in place to help ensure that the system performs according to specifications and that new development does not adversely impact existing functionality.

Each software change undergoes stringent and extensive testing prior to release, where our experienced programmers test system modifications before passing them on to trained quality assurance staff for further testing. Documentation is reviewed for accuracy prior to publication.

Protection of Record Data

The majority of Epic's fields are populated through pre-defined category lists and master file records, ensuring valid data entry. The system also prevents entry of invalid data formats in standard fields and in responses to custom questionnaires (free text in a date field, for example).

Epic's system prevents modifications to signed inpatient notes and ambulatory progress notes, closed ambulatory encounter records, reviewed discharge instructions, and letters marked as "Sent." If needed, notes, discharge instructions, and encounters can be updated using the Addendum feature in EpicCare®. This feature clearly indicates within an encounter or clinical note that the text has been updated and provides a link to the original visit narrative or inpatient note.

Generation of Hard Copy and Electronic Records

EpicCare's numerous standard Print Groups pull a full range of clinical and demographic information into printable patient summary reports, which include a configurable Master Summary report. Print Groups pull information from the underlying database in real time, so when reports are selected they display the most current data. The EpicWeb® and AffiliateLink® applications provide a secure Web-based method for record review.

Epic's reporting tools give you the ability to make aggregate patient data analyses available in a variety of electronic formats. Reports created using the Clarity® component of the Clarity/Analyst® Enterprise Reporting System query data extracted to a separate reporting database, to avoid impacting production operations. These extracts can occur nightly.

Support for Timely Retrieval of Accurate Records

Epic's system uses an enterprise-wide data repository and, with the proper hardware configuration, requires no data archiving or purging, ensuring that complete electronic patient records are immediately available to authorized users. With the proper hardware configuration our system is highly available; our standard hardware recommendations include redundancy and high availability components that supplement highly available operating system software.

System access controls

Individuals must authenticate their identities at login to access the system. The standard authentication mechanism is a unique ID-password combination. Epic uses a modular approach to support other authentication mechanisms, where ActiveX components can be switched in to support the devices deployed at the client site. This allows you to use options such as proximity badges, card swipes, secure-ID cards, fingerprint readers or other biometric devices, or a combination of these techniques. An open authentication structure enables the system to employ server-based authentication via directory services such as Microsoft Active Directory or Novell eDirectory.

Epic's system can inactivate a user record after a specified number of unsuccessful login attempts. This setting can be different for long term (days) and short term (minutes) attempts, and administrators can determine whether to count only cumulative failed attempts.

Audit trails

Epic provides a comprehensive audit trail that includes the user ID, date and time of access, and contact record accessed. Examples of actions the EpicCare Enterprise Clinical System automatically date-, time-, and user-stamps include:

- Signing or cosigning an order
- Canceling an order
- Marking a result report as "Done"
- Linking a scanned image to the patient's record
- Acknowledging inpatient orders
- Filing a nursing note or progress note for an ambulatory encounter
- Filing or cosigning an inpatient note
- Charting against goals and recording variances for inpatient care plans
- Closing or cosigning an ambulatory encounter
- Entering flowsheet data
- Identifying discharge instructions as Pended or Reviewed.

The EpicCare record also includes times documented for medication administration, inpatient instruction, dispositions of telephone encounters, and ABN updates. The system captures the times interfaced results are received.

The system preserves a view-only history of a patient's allergy and chronic medical problem data, identifying each update by entry person and date. Updates to inpatient notes, discharge summaries, and encounter narratives documented through the Addendum feature do not overwrite the original text.

Epic's Access History utility logs events, which roughly correspond to secured functions of the software. When a user with the proper authorization executes a function that allows him or her to view certain data, the software records an Access History event. Access History data can be extracted to a reporting database for analysis.

Epic's Chronicles® Edit Trails can be activated to provide additional tracking for specific data elements. When the value of one of these data elements is changed, the Edit Trail captures the update, the user, the instant of update, and the previous data value.

With the appropriate hardware configuration, Epic's database can maintain audit trail data indefinitely.

SEQUENCING RULES

Epic's use of required fields and configurable Order Validation/Close Visit Validation checks provide the ability to prevent a user from signing an order or closing an encounter before required information is documented. The system's multi-step order transmittal function routes orders to user In Baskets for additional documentation according to a specified sequence before sending the orders to be resulted. Transcribed notes are not filed to the patient's permanent record prior to provider approval, and you can require residents to forward transcriptions to a supervisor for final approval.

SYSTEM FUNCTIONALITY CONTROLS

Epic manages user access to information and functionality via User Records in its database, where access privileges are determined by the User Roles and Security Classifications assigned to users in these database records. User Roles determine what options and workflows are available to users and Security Classifications provide more granular controls, with security checkpoints that determine whether a user can access specific functions. You have the option of assigning users separate Security Classifications that correspond to different areas where those users work.

Other examples of Epic's security and confidentiality controls include:

- Profiles that determine what Patient Summary reports are available to users and allow you to create role-specific views of data based on encounter types.
- The Break-the-Glass feature for determining appropriate contexts for access to "views" or sets of information within the record. Context checks can apply to views in the entire record or to contacts that meet certain criteria (for example, the contact involves a certain department or is within a certain date range).

  If a user needs to access record information outside of an allowed context, he or she can "break the glass" in order to gain emergency access. You can configure the system to produce a comprehensive audit report and send a notification to appropriate personnel when a "break the glass" access occurs.
- Authorized users can mark individual patient records as 'restricted' to prevent general access to VIP or employee information. Only users with security for restricted records can view information related to these patients.
- EpicCare supports sensitive orders and encounters, which can only be accessed by the documenting physician, that physician's supervisor, and designated proxies.

Device checks

A workstation, thin client, laptop, or tablet must be registered in Epic's database in order for the user to access the system. Epic's open authentication structure gives you the ability to use biometric devices to validate users' identities when they log in.

Epic development and support staff training

Epic actively recruits the brightest industry professionals and graduates from top colleges around the country, conducting meticulous evaluation and testing before hiring an applicant. Our new hires are assigned mentors and follow a carefully scripted orientation program that provides training in how to perform their assigned tasks.

In addition to the schedule of orientation classes, development and support staff members are required to take application training and achieve high scores on a number of certification tests. Once the initial orientation program and camps are complete, they begin focused assignments and an additional set of advanced technical training classes relevant to their roles.

You will determine what qualifications are required for personnel employed by your organization who configure, support, or use Epic's system. Epic offers a comprehensive training curriculum and a certification program for your project team. In addition to application functionality and administration courses, available classes include Clarity Clinical Reporting, Training, Environments, and Documentation; Interface Administrator, Workstation System Manager, Overview of Epic Implementation, and others. New Version Training courses for your project team enable your staff to remain current on upgrades to Epic software.

Documentation of system modifications

As development begins on a new version of Epic's system, programs and other objects under development are linked to automated tracking logs. The logs indicate the nature of the changes being made, serve as check-out mechanisms so that only one programmer can be modifying the object, and track the object's progress through the development, programmer code review, quality assurance testing, and release processes.

Epic's change control methodology for development performed in a client's system includes a formal Release Authorization process that requires us to receive sign-off from you before any system changes are made or application objects are delivered to any of your environments. This provides a clear record of the changes Epic has applied to your system.

Epic identifies system changes in release notes it makes available with major releases and Monthly Updates. Epic's system documentation is available in Microsoft Word format, and you can use Word's Compare Documents feature to identify updates and modifications made to the content of the documentation since the previous release.

User and patient signature information

The "Audit trails" section on page 6 of this paper indicates some of the functions in EpicCare where the system captures the name of the user who executed an action, and the date and time the action was executed. EpicCare automatically captures user information when the listed

functions are performed, and the system can prompt the user for password re-entry at these and other points in a clinical workflow.

Epic's registration and clinical applications support patient electronic signature capture for association with electronic documents, when used with the appropriate hardware. The record of an electronic patient signature can indicate the date and time the document was signed.

User and patient signatures are available for electronic display in the patient's record. Where needed, Epic has developed Print Groups for displaying user signatures in printed records.

Incorporation of Signatures into Appropriate Records

User signatures and links to patient signatures are embedded in their associated records, and cannot be copied or transferred to other records.

Electronic Signatures

Epic's system automatically assigns each user a unique ID, and this ID in combination with that user's password or biometric identification functions as the user's signature.

Signature controls

Epic's standard user validation mechanism for allowing system access is entry of the user's ID and password. You can require password re-authentication at key points in the workflow, such as signing orders. Epic uses a modular approach to support third party biometric authentication mechanisms, where ActiveX components can be switched in to support the devices employed.

ID and password controls

Each user has a unique ID in Epic's system. Password administrators can:

- Force passwords to expire after a specified number of days, varying this time period for individual users if needed.
- Replace a user's password in situations where the password is compromised.
- Control the format of user passwords.
- Determine whether staff members can reuse passwords.
- Force individual users to change their passwords the next time they log in. Administrators can also run a routine that forces password changes for groups of users.

Epic's system provides optional limitations on user access, which can guard against unauthorized uses of identification codes. These limitations are defined in user records, allowing you to vary these limitations for different users.

- User access can be restricted to specific times of day and days of the week. Holidays may be included or excluded.
- Users can be given start and end dates which limit the time periods over which they have access to the system.
- A user's record can be deactivated after a specified number of days have elapsed since the user last logged in.
- The number of simultaneous logins a user is allowed can be restricted.