| **Section/ID#:**  **Type:**  **Name:** | **Conformance Criteria** | **See**  **Also** |
| --- | --- | --- |
| **IN.2.1 – Record Lifecycle**  **IN.2.2 – Record Lifespan** |  | **Function**  **Level**  **See Also** |
| **Header** |
| **Manage Record Lifecycle and Lifespan** |
| Actions are taken to support patient health. Actions are taken in provision of healthcare to individuals. Actions are taken as the result of rules-based EHR System algorithms. Actors (i.e., patients, providers, users, systems) take Actions. (Actions broadly encompass tasks, acts, procedures or services performed or provided.)  Actions have corresponding Entries in the EHR Record, i.e., Action instances correspond to Record Entry instances. These Record Entries provide persistent evidence of Action occurrence, context, disposition, facts, findings and observations. The EHRS Functional Model does not specify a particular relationship of Actions and corresponding Record Entries. It may be one to one, many to one or even one to many.  Actions have associated metadata (e.g., who, what, when, where, why, how, under what conditions, in what context). The corresponding Record Entry captures this metadata along with other Action and Record Entry related information. Record Entries may be encapsulated to bind author/system/time signatures to data and metadata content.  Each Record Entry also includes its own provenance metadata such as who (author) and when (documented). The EHR System captures Actions taken and creates corresponding Record Entries. The EHR System subsequently manages those Entries, according to scope of practice, organizational policy and jurisdictional law.  Record Entries may be created during the course of the Action or Record Entries may be created sometime thereafter. The Actor/Source of the Record Entry may be the same as an Actor performing the Action or not.  Actions and related Record Entries capture a chronology of patient health and healthcare and also a chronology of operations and services provided in a healthcare enterprise. Record Entries reflect changes in health information from the time it was created, to the time it was amended, sent, received, etc. In this manner, each Record Entry serves as persistent evidence of an Action taken, enabling providers to maintain comprehensive information that may be needed for legal, business, and disclosure purposes. To satisfy these purposes, Record Entries must also be retained and persisted without alteration.  Record Entries have both a lifecycle and a lifespan. Lifecycle Events include originate/retain, amend, verify, attest, access/view, transmit/receive, and more. Lifecycle Events occur at various points in a Record Entry lifespan, always starting with a point of origination and retention (i.e., when the Entry is first created and stored).  A Record Entry may have a pre and post Event state if content is modified. In this case, the original Record Entry is preserved (with signature binding) and a new Entry is created (with new signature binding).  A Record Entry contains data and metadata, in multiple formats, following various conventions and standards. Included are tagged and delimited data, structured (concise, encoded), unstructured (free form), data formatted as text, documents, images, audio, waveforms, in ASCII, binary or other encoding.  Record Lifecycle Events also Initiate a corresponding Audit Trigger and Audit Log Entry (see IN.12.1.1). The EHR System manages Record Lifecycle Events for each Record Entry, including pre and post Event record states, continuity, persistence and related Record Audit Logs.  Action examples include: (1) In the direct care of a patient, a healthcare professional creates or amends health information to be contained in a history and physical; (2) A medical device can supply the EHR system with a test result; (3) The EHR system can alert the healthcare professional of a potential drug-drug interaction.  As described here, Record Lifecycle Events are those required to manage Record Entries in persistent storage over the full course of Record Lifespan. | |  |
| **IN.2.1** |  | **Function**  **Level**  **See Also** |
| **Header** |
| **Record Lifecycle** |
| **Statement:**  Manage Record Lifecycle  **Description:**  As above  **References:**  **ISO 21089 – Health Informatics – Trusted End-to-End Information Flows**  **HL7 Electronic Health Record Lifecycle Model DSTU** | 1. The system **SHALL** conform to Section IN.2.2.1, Manage/Persist Record Entry, as the final step to conclude each Record Lifecycle Event in Section IN.2.1. |  |
|  |  |
| **IN.2.1.1** | ~~DC.1, DC.1.1.1, DC.1.1.3.2, DC.1.3.3, DC.1.8.4, DC.1.8.5, DC.2, DC.2.3.2, DC.2.4.5.1-2, DC.3, DC.3.1.1, DC.3.1.3, DC.3.2.2.4, S.1, S.2, S.3, IN.1.1, IN.1.2, IN.1.3, IN.1.5, IN.1.8,~~  ~~IN.1.9, IN.2.1, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Originate and Retain Record Entry** |
| **Statement:**  Originate and Retain a Record Entry (1 instance)  **Description:**  Occurs when Record Entry is originated – typically during the course of an Action itself, to document the Action and context.  • An identified Author or Source is responsible for Record Entry content.  • Record Entry contains Metadata about the Action and its circumstances, e.g., who, what, when, where, facts, findings, observations, etc.  • An Audit Trigger is initiated to track Record Entry origination and retention.  **Reference: ISO 21089, Section 12.2.2.** | 1. The system **SHALL** provide the ability to create (originate) a Record Entry instance corresponding to an Action instance and context. |  |
| 2. The system **SHALL** create a unique instance identifier for each Record Entry. |  |
| 3. The system **SHALL** conform to Section IN.12.1.1.1, Originate/Retain Record Entry Audit Trigger. |  |
| 4. The system **SHALL** capture the full set of identity, event and provenance Audit Metadata, conforming to Section IN.12.1.1.1. |  |
| 5. The system **SHALL** capture the signature event (e.g., digital signature) of the origination entry Author, binding signature to Record Entry content. |  |
| 6. The system **SHALL** provide the ability to capture both structured and unstructured content in Record Entries. |  |
| 7. The system **SHALL** provide the ability to create Record Entries from information captured during system downtime. |  |
| 8. The system **SHOULD** provide the ability to integrate Record Entries from Information captured during system downtime. |  |
| 9. The system **SHALL** provide the ability to capture date/time of an Action was taken or data was collected if different than date/time of the Record Entry. |  |
| 10. The system **SHOULD** capture metadata that identifies the source of non-originated Record Entry (e.g., templated, copied, duplicated, or boilerplate information). |  |
| 11. The system **MAY** provide the ability to tag unstructured Record Entry content to organize it according to need, for example, in a time-related fashion, by application-specific groups (such as photographs, handwritten notes, or auditory sounds), or by order of relative importance. |  |
| 12. The system **MAY** create and internalize the Record Entry encoded as a standards-based data object (e.g., HL7 Continuity of Care or other HL7 CDA R2 Document). |  |
| 13. The system **MAY** create a standards-based data object to mirror (be duplicate and synchronous with) internal Record Entry representation. |  |
|  |  |
| **IN.2.1.2** | ~~DC.1, DC.1.1.1, DC.1.1.3.2, DC.1.3.3, DC.1.8.4, DC.1.8.5, DC.2, DC.2.3.2, DC.2.4.5.1-2, DC.3, DC.3.1.1, DC.3.1.3, DC.3.2.2-4, S.1, S.2, S.3, S.3.1.5, IN.1.1, IN.1.2, IN.1.3, IN.1.5, IN.1.8, IN.1.9, IN.2.1, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Amend Record Entry Content** |
| **Statement:**  Amend content of an Record Entry (1 instance)  **Description:**  Occurs when Record Entry content is modified (from its original or previously retained state) – typically upon conclusion of an Action, to correct, update or complete content.  • Amended Record Entry content is the responsibility of authorized amendment Author(s).  • The amendment becomes part of the Act Record revision history, where the original content and any  previous amendments are retained without alteration.  • After amendment, the System is responsible for retention of the Record Entry and its revision history.  • An Audit Trigger is initiated to track Record Entry amendment.  **Reference: ISO 21089, Section 12.3.2** | 1. The system **SHALL** provide the ability to amend Record Entry content. |  |
| 2. The system **SHALL** retain the original and all previously amended versions of the Record Entry, without alteration. |  |
| 3. The system **SHALL** create a new uniquely identifiable version of the Record Entry, incorporating amended content. |  |
| 4. The system **SHALL** conform to Section IN.12.1.1.2, Amend Record Entry Audit Trigger. |  |
| 5. The system **SHALL** capture the full set of identity, event and provenance Audit Metadata, conforming to Section IN.12.1.1.2. |  |
| 6. The system **SHALL** capture the signature event (e.g., digital signature) of the amendment Author, binding signature to Record Entry content. |  |
| 7. The system **SHALL** capture the reason for amendment as Audit Metadata, as per Section IN.12.1.1.2, e.g., to add information, to correct erroneous information or to augment/supplement Record Entry. |  |
| **IN.2.1.3** | ~~DC.1, DC.2, DC.3, S.1, S.2, S.3, S.3.1.5, IN.1.1, IN.1.2, IN.1.3, IN.1.5, IN.1.8, IN.1.9, IN.2.2, IN.2.5.1-2, IN.4.1-3, IN.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Translate Record Entry Content** |
| **Statement:**  Translate content of Record Entries (1 or more instances)  **Description:**  Occurs when Record Entries are amended to include translation of content – typically to transform coded data  from one coding/classification scheme to another, also from one human language to another.  • Translated (amended) Record Entry content is the responsibility of translating System – which invokes  mapping/translation rules for each relevant record attribute.  • The translation amendment becomes part of the Record Entry revision history, where original content and  any previous amendments are retained without alteration.  • After translation amendment, the System is responsible for retention of the Record Entry and its revision  history (including the translation event).  • An Audit Trigger is initiated to track Record Entry translation.  **Reference: ISO 21089, Sections 12.3.2 and 12.4.** | 1. The system **SHOULD** provide the ability to translate coded Record Entry content from one coding/classification system to another. |  |
| 2. The system **SHOULD** provide the ability to translate coded Record Entry content from one value set to another. |  |
| 3. The system **MAY** provide the ability to translate Record Entry content from one human language to another. |  |
| 4. The system **SHOULD** retain the original and all previously amended versions of the Record Entry, without alteration. |  |
| 5. The system **SHOULD** create a new uniquely identifiable version of the Record Entry, incorporating translated content. |  |
| 6. The system **SHOULD** conform to Section IN.12.1.1.3, Translate Record Entry Audit Trigger. |  |
| 7. The system **SHOULD** capture the full set of identity, event and provenance Audit Metadata, conforming to Section IN.12.1.1.3. |  |
| **IN.2.1.4** | ~~DC.1, DC.1.8.3, DC.2, DC.3, S.1, S.2, S.3, IN.1.1, IN.1.2, IN.1.3, IN.1.5, IN.1.8, IN.1.9, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Attest Record Entry Content** |
| **Statement:**  Attest to content of Record Entry (1 instance)  **Description:**  Occurs when Record Entry content is attested for accuracy and completeness – typically during/after conclusion of an Action.  • Attested Record Entry content is the responsibility of Attesting Author. The Attesting Author may be someone other than the originating Author, i.e., a supervisor, proctor, preceptor or other designated individual.  • An Audit Trigger is initiated to track Record Entry attestation.  **Reference: ISO 21089, Section 12.2.2.** | 1. The system **SHALL** provide the ability to attest Record Entry content. |  |
| 2. The system **SHALL** conform to Section IN.12.1.1.4, Attest Record Entry Audit Trigger. |
| 3. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.4. |
| 4. The system **SHALL** capture the signature event (e.g., digital signature) of the Attesting Author, binding signature to Record Entry content. |
| **IN.2.1.5** | ~~DC.1, DC.1.1.3.1, DC.1.1.4, DC.1.1.5, DC.1.8.3, DC.1.8.5, DC.2, DC.3, S.1, S.2, S.3, IN.1.1, IN.1.2, IN.1.3, IN.1.5, IN.1.9, IN.2.1, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **View/Access Record Entry Content** |
| **Statement:**  View/Access content of Record Entries (1 or more instances)  **Description:**  Occurs when Record Entries are viewed or accessed.  • Viewed Record Entry content is the responsibility of authorized User(s).  • An Audit Trigger is initiated to track Record Entry views and access.  **Reference: ISO 21089, Section 12.5.** | 1. The system **MAY** embed masks to limit view/access of Record Entry content to authorized individuals. |  |
| 2. The system **SHALL** provide the ability to view/access Record Entry content, including original version and any subsequent amendments. |  |
| 3. The system **SHALL** provide the ability to view/access Record Entry content down to the discrete element or item, including encoded fields. |  |
| 4. The system **SHALL** conform to Section IN.12.1.1.5, View/Access Record Entry Audit Trigger. |  |
| 5. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.5. |  |
| **IN.2.1.6** | ~~DC.1, DC.2, DC.3, DC.3.1.1, DC.3.1.3, DC.3.2.2-4, S.1, S.2, S.2.1.2, S.2.2, S.2.2.1-3, S.3, S.3.3.3-6, S.3.6, IN.1.1, IN.1.2, IN.1.6, IN,1.7, IN.1.9, IN.2.1, IN.2.2, IN.2.3, IN.2.5.1-2, IN.4.1-3, IN.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Transmit and/or Disclose Record Entries** |
| **Statement:**  Transmit/Disclose content of Record Entries (1 or more instances)  **Description:**  Occurs when Record Entry content is transmitted and/or disclosed – typically to an external entity or system.  • Transmittal may include original Record Entry content with subsequent amendment(s), if any.  • Transmittal of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry transmittal and disclosure.  **Reference: ISO 21089, Section 12.8.1.** | 1. The system **SHOULD** provide the ability to transmit Record Entry content to external systems, retaining original, unaltered content and signature bindings, Action and Record Entry provenance and metadata. |  |
| 2. The system **SHALL** provide the ability to transmit Record Entry extracts to external systems, including content, context, provenance and metadata. |  |
| 3. The system **SHALL** identify the patient or individual subject of transmitted/disclosed Record Entry content. |  |
| 4. The system **SHALL** create a log entry for disclosure of protected Record Entry content, according to organizational policy and jurisdictional law. |  |
| 5. If a specific recipient is known, the system **SHOULD** disclose protected Record Entry content according to established permissions, organizational policy and jurisdictional law. |  |
| 6. If known and explicit as to Record Entry content being transmitted, the system **SHOULD** transmit corresponding authorizations and patient consent permissions. |  |
| 7. The system **SHALL** conform to Section IN.12.1.1.6, Transmit/Disclose Record Entry Audit Trigger. |  |
| 8. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.6. |  |
| 9. The system **SHALL** conform to Section IN.1.6, Secure Data Exchange. |  |
| 10. The system **SHALL** provide the ability to extract Record Entry content prior to transmittal/disclosure, conforming to Section IN.2.1.11, Extract Record Entry Content. |  |
| 11. The system **SHALL** provide the ability to de-identify Record Entry content prior to transmittal/disclosure, conforming to Section IN.2.1.8, De-Identify Record Entries. |  |
| 12. The system **SHALL** provide the ability to transmit updates (new versions) of Record Entry Content to known recipients of prior versions according to organizational policy and jurisdictional law. |  |
| 13. The system **SHALL** provide the ability to transmit with each exchange the most recent or all versions of Record Entry Content depending on organizational policy and jurisdictional law. |  |
| **IN.2.1.7** | ~~DC.1, DC.2, DC.3, DC.3.1.1, DC.3.1.3, DC.3.2.2-4, S.1, S.2, S.2.1.2, S.2.2, S.2.2.1-3, S.3, S.3.3.3-6, S.3.6, IN.1.1, IN.1.2, IN.1.6, IN,1.7, IN.1.9, IN.2.1, IN.2.2, IN.2.3, IN.2.5.1-2, IN.4.1-3, IN.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Receive and Retain Record Entries** |
| **Statement:**  Receive and retain/persist content of Record Entries (1 or more instances)  **Description:**  Occurs when Record Entry content is received **–** typically from an external system.  • Receipt of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry receipt and retention.  **Reference: ISO 21089, Section 12.8.1.** | 1. The system **SHOULD** provide the ability to receive and retain/persist Record Entry content from external systems, retaining original unaltered content and signature bindings, Action and Record Entry provenance and metadata. |  |
| 2. The system **SHALL** provide the ability to receive and retain/persist Record Entry extracts from external systems, including source, identity, record content, corresponding provenance and metadata. |  |
| 3. The system **SHALL** identify the patient or individual subject of received Record Entry content. |  |
| 4. If received with Record Entry content, the system **SHOULD** limit subsequent data access to that permitted by corresponding authorizations and patient consents. |  |
| 5. The system **SHALL** conform to Section IN.12.1.1.7, Receive/Retain Record Entry Audit Trigger. |  |
| 6. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.7. |  |
| **IN.2.1.8** | ~~S.1.5, S.2, S.2.2, IN.1.1, IN.1.2, IN.1.9, IN.2.1, IN.2.2, IN.2.3, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **De-identify Record Entries** |
| **Statement:**  De-identify content of Record Entries (1 or more instances)  **Description:**  Occurs when Record Entry content is transformed into de-identified version.  • De-identification of Record Entries may be initiated by User command.  • De-identification of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry de-identification.  **Reference: ISO 21089, Section 12.6.1.** | 1. The system **SHALL** provide the ability to de-identify Record Entry content according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** conform to Section IN.12.1.1.8, De-Identify Record Entry Audit Trigger. |  |
| 3. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.8. |  |
| **IN.2.1.9** | ~~S.1.5, S.2, S.2.2, IN.1.1, IN.1.2, IN.1.9, IN.2.1, IN.2.2, IN.2.3, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Pseudo-Nominize Record Entries** |
| **Statement:**  Provide pseudo-nominized identity for Record Entries (1 or more instances)  **Description:**  Occurs when Record Entry is transformed into an pseudo-nominized version.  • Pseudo-nominization allows records to be later re-identified.  • Pseudo-nominization of Record Entries may be initiated by User command.  • Pseudo-nominization of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry pseudo-nominization.  **Reference: ISO 21089, Section 12.6.1.** | 1. The system **SHALL** provide the ability to pseudo-nonimize (or associate new identity with) patient Record Entries according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** conform to Section IN.12.1.1.9, Pseudo-Nominize Record Entry Audit Trigger. |  |
| 3. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.9. |  |
| **IN.2.1.10** | ~~IN.1.1, IN.1.2, IN.1.9, IN.2.2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Re-identify Record Entries** |
| **Statement:**  Re-identify previously aliased identity for content of Record Entries (1 or more instances)  **Description:**  Occurs when Record Entries are re-identified from a previously aliased version.  • Re-identification of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry re-identification.  **ISO 21089, Section 12.6.2.** | 1. The system **SHALL** provide the ability to re-identify (or associate original identity with) Record Entry content according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** conform to Section IN.12.1.1.10, Re-Identify Record Entry Audit Trigger. |  |
| 3. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.10. |  |
| **IN.2.1.11** | None specified | **Function**  **Level**  **See Also** |
| **Header** |
| **Extract Record Entry Content** |
| **Statement:**  Extract Record Entry content to produce subsets, derivations, summaries or aggregations (Multiple instances)  **Description:**  Occurs when Record Entry content is extracted to render subsets, derivations, summaries or aggregations.  • Extraction of Record Entry content may be initiated by User command and/or rules-based algorithm.  • Extraction of Record Entry content is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry content extraction.  **ISO 21089, Section 12.7.** | 1. The system **SHALL** provide the ability to extract Record Entry content to produce subsets, derivations, summaries or aggregations according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** provide the ability to de-identify Record Entries during extraction in accordance with Section IN.2.1.8, De-Identify Record Entries. |  |
| 3. The system **SHALL** provide the ability to extract Record Entry content based on queries with selection criteria, for example, key words, date/time range, full text search. |  |
| 4. The system **SHALL** provide the ability to extract metadata associated with Record Entry content. |  |
| 5. The system **SHOULD** provide the ability to extract, with parameterized selection criteria, across the complete data set that constitutes all Record Entries for a patient. |  |
| 6. The system **SHOULD** provide the ability to extract and present a full chronicle of the healthcare process from assembled Record Entries. |  |
| 7. The system **SHOULD** provide the ability to extract and present a full chronicle of healthcare delivered to a patient from assembled Record Entries. |  |
| 8. The system **SHALL** provide the ability to extract Record Entry content for various purposes, including administrative, financial, research, quality analysis and public health. |  |
| 9. The system **SHOULD** provide the ability to extract Record Entries for system migration. |  |
| 10. The system **SHOULD** provide the ability to specify over-riding parameters to exclude sensitive or privileged Record Entry content from extraction. |  |
| 11. The system **MAY** provide the ability to extract unstructured Record Entry content and convert it into structured data. |  |
| 12. The system **SHALL** conform to Section IN.12.1.1.11, Extract Record Entry Audit Trigger. |  |
| 13. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.11. |  |
| **IN.2.1.12** | ~~DC.1.1.1, IN.1.1, IN.1.2, IN.2.1, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Archive Record Entries** |
| **Statement:**  Archive Record Entries (1 or more instances)  **Description:**  Occurs when Record Entries are archived – typically to off-line (less readily available) storage media.  • Archival of Record Entries may be initiated by User command.  • Archival of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry archival.  **ISO 21089, Section 12.10.** | 1. The system **SHALL** provide the ability to manage archival of Record Entries to off-line or near-line media according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** provide the ability to configure archival parameters for Record Entries (e.g., what and when to archive). |  |
| 3. The system **SHALL** archive Record Entries according to Section IN.8, Archive and Retrieval. |  |
| 4. The system **SHALL** conform to Section IN.12.1.1.12, Archive Record Entry Audit Trigger. |  |
| 5. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.12. |  |
| **IN.2.1.13** | ~~S.2.2, IN.1.1, IN.1.2, IN.2.1, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Destroy or Identify Record Entries as Missing** |
| **Statement:**  Destroy or Identify Record Entries as Missing (1 or more instances)  **Description:**  Occurs when Record Entries are destroyed or identified as missing.  • Destruction typically occurs after conclusion of the legal retention period.  • Destruction of Record Entries may be initiated by User command.  • Destruction of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry Destruction or Notation as Missing.  **ISO 21089, Section 12.11.** | 1. The system **SHALL** provide the ability to destroy Record Entries (e.g., those exceeding their legal retention period) according to organizational policy and/or jurisdictional law. |  |
| 2. The system **MAY** provide the ability to restore (reverse, re-activate) previously destroyed Record Entries. |  |
| 3. The system **SHALL** provide the ability to identify Record Entries as missing. |  |
| 4. The system **SHALL** conform to Section IN.12.1.1.13, Destroy Record Entry Audit Trigger. |  |
| 5. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.13. |  |
| **IN.2.1.14** | ~~DC1.1.1~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Deprecate Record Entries** |
| **Statement:**  Deprecate Record Entries as invalid (1 or more instances)  **Description:**  Occurs when Record Entries are deprecated if found to be improperly identified or otherwise invalid.  • Deprecation of Record Entries may be initiated by User command.  • Deprecation of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry Deprecation. | 1. The system **SHALL** provide the ability to deprecate Record Entries as invalid according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** conform to Section IN.12.1.1.14, Deprecate Record Entry Audit Trigger. |  |
| 3. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.14. |  |
| **IN.2.1.15** |  | **Function**  **Level**  **See Also** |
| **Header** |
| **Re-Activate Record Entries** |
| **Statement:**  Re-activate Record Entries (1 or more instances)  **Description:**  Occurs when Record Entries are made active again after previously Destroy or Deprecate.  • Re-activation of Record Entries may be initiated by User command.  • Re-activation of Record Entries is the responsibility of the System – which invokes relevant rules.  • An Audit Trigger is initiated to track Record Entry Re-Activation. | 1. The system **SHALL** provide the ability to re-activate (previously destroyed or deprecated) Record Entries according to organizational policy and/or jurisdictional law. |  |
| 2. The system **SHALL** conform to Section IN.12.1.1.15, Re-Activate Record Entry Audit Trigger. |  |
| 3. The system **SHALL** capture the full set of identity and event Audit Metadata, conforming to Section IN.12.1.1.15. |  |

|  |  |  |
| --- | --- | --- |
| **IN.2.2.1** | ~~DC.1, DC.1.1.1, DC.1.1.3.2, DC.1.3.3, DC.1.8.4, DC.1.8.5, DC.2, DC.2.3.2, DC.2.4.5.1-2, DC.3, DC.3.1.1, DC.3.1.3, DC.3.2.2-4, S.1, S.2, S.3, S.3.1.5, IN.1.1, IN.1.2, IN.1.3, IN.1.5, IN.1.8, IN.1.9, IN.2.1, IN.2.2, IN.2.5.1-2~~ | **Function**  **Level**  **See Also** |
| **Header** |
| **Manage Record Entries** |
| **Statement:**  Manage/Persist Record Entries (Multiple instances)  **Description:**  Occurs upon Record Entry origination/retention and thereafter on a continuous and uninterrupted basis for lifespan of each Record Entry.  • Ensures long-term retention and preservation of EHR Record Entries, without alteration.  **Reference: ISO 21089, Section 12.2.2** | 1. The system **SHALL** manage each Record Entry as a persistent, indelible (unalterable) data object, including its revision history. |  |
| 2. The system **SHALL** manage (persist) each Record Entry for its applicable retention period according to scope of practice, organizational policy and jurisdictional law. |  |
| 3. The system **SHALL** manage (persist) the full set of identity, event and provenance Audit Metadata for each Record Entry, conforming to Section IN.12.1.1, Record Entry Audit Triggers. |  |
| 4. The system **SHALL** manage (persist) the signature event (e.g., digital signature) of each Record Entry. |  |
| 5. The system **SHALL** manage Record Entries with data content in standard and non-standard formats. |  |
| 6. The system **SHALL** manage Record Entries containing both structured and unstructured data. |  |
| 7. The system **SHOULD** manage Record Entry content with tagged or delimited elements including data formatted as text, documents, images, audio, waveforms, in ASCII, binary and other encodings. |  |
| 8. The system **SHOULD** manage Record Entries in clinical and business contexts. |  |
| 9. The system **SHOULD** provide the ability to specify sets of clinical and business context data, to be captured in or linked to Record Entries. |  |
| 10. The system **SHOULD** provide the ability to retrieve all available elements included in the definition of a legal medical record (including Audit Log Entries and the decoded translation of anything stored only in code form) in accordance with user scope of practice, organizational policy and/or jurisdictional law. |  |
| 11. The system **MAY** (automatically or manually) provide the ability to tag specific Record Entries for deletion according to user scope of practice, organizational policy and/or jurisdictional law. |  |
| 12. IF allowing tags for specific Record Entry deletion, THEN the system **SHALL** provide the ability to review and confirm the set of tagged Entries before actual deletion occurs according to user scope of practice, organizational policy and/or jurisdictional law. |  |
| 13. IF allowing tags for specific Record Entry deletion, THEN the system **SHALL** provide the ability to delete Entries according to user scope of practice, organizational policy and/or jurisdictional law. |  |
| 14. IF allowing tags for specific Record Entry deletion, THEN the system **SHALL** provide the ability to confirm that the destruction occurred according to user scope of practice, organizational policy and/or jurisdictional law. |  |
| 15. The system **MAY** provide the ability to undelete Record Entries according to user scope of practice, organizational policy and/or jurisdictional law. |  |
| 16. The system **MAY** transmit record destruction date information along with existing data when transmitting Record Entries (or extracts) to another entity. |  |
| 17. The system **SHOULD** manage health care information for organizations that have multiple facilities according to scope of practice. |  |
|  |  |
| **IN.2.2.2** |  | **Function**  **Level**  **See Also** |
| **Header** |
| **Manage Record Entries for Legal Hold** |
| **SHOULD THIS BE A LIFECYCLE EVENT?** | | |
| **Statement:**  Manage/Preserve Record Entries for Legal Hold (Multiple instances)  **Description:**  Occurs when a set of Record Entries is designated to be held for legal purposes or proceedings.  • Ensures preservation of a set of Record Entries for a designated time, held without alteration.  **Reference: ISO 21089, Section 12.2.2** | 1. The system **SHOULD** provide the ability to secure data/records from un-auditable alteration or unauthorized use for preservation purposes such as a legal hold. |  |
| 2. The system **SHALL** provide the ability to preserve records beyond normal retention period according to organizational policy or jurisdictional law. |  |
| 3. The system **SHOULD** provide the ability to identify the reason for preserving records beyond the normal retention period. |  |
| 4. The system **SHOULD** provide the ability to generate a legal hold notice identifying who to contact for questions when a user attempts to alter a record on legal hold. |  |
| 5. The system **MAY** map medical record elements to the metadata to provide the business context, conforming to IN.2.2.1, Manage Record Entries, Conformance Criteria 7-8. |  |
| 6. The system **MAY** provide the ability to render Record Entry content preserved for a legal hold by type, class or encounter (for example: medical record entry or report, e-mail, metadata, etc.), conforming to Section IN.2.1.11, Extract Record Entry Content. |  |