HL7 Electronic Health Record Work Group
EHR System Functional Model Release 2 – Record Infrastructure – Record Lifecycle Event Metadata on FHIR
DRAFT FHIR Code/Value Set Analysis, Comments, Proposals – 23 September 2014

Blue = proposed additions Red = resource attributes and code/value sets identified as Record Lifecycle Event Metadata

Resource Attribute	Description	Code/Value: Description	Notes or Proposal
Resource – Provenance – Who, What, When for a set of resources			
reason : CodeableConcept 0..1	Reason activity is occurring	TBD	
Resource – Provenance Agent 0..* – Person, organization, records, etc. involved in creating resource			
role : Coding 1..1 « ProvenanceAgentRole+ »	e.g. author | overseer | enterer | attester | source | cc	Enterer: A person entering the data into the originating system Performer: A person, animal, organization or device that who actually and principally carries out the activity Author: A party that originates the resource and therefore has responsibility for the information given in the resource and ownership of this resource Verifier: A person who verifies the correctness and appropriateness of activity Attester: A verifier who attests to the accuracy of the resource Informant: A person who reported information that contributed to the resource Source: An information source from which the portions of the resource are derived Cc: A party, who may or should receive or who has received a copy of the resource or subsequent or derivative information of that resource Application: An application with a user interface that interacts with a person Daemon: A background process that transfers information from one place or form to another	
type : Coding 1..1 « ProvenanceAgentType + »	e.g. Resource | Person | Application | Record | Document	Person: The participant is a person acting on their on behalf or on behalf of the patient rather than as an practitioner for an organization. I.e. "not a healthcare provider" Practitioner: The participant is a practitioner Organization: The participant is an organization Software: The participant is a software application Record: The participant is a logical record. The record itself participated in the activity Document: The participant is a document	

Resource Attribute	Description	Code/Value: Description	Notes or Proposal
Resource – SecurityEvent.Event 1..1 – What was done			
type : CodeableConcept 1..1 « SecurityEventType+ »	Type/identifier of event	Rest + DICOM codeset	
subtype : CodeableConcept 0..* « SecurityEventSubType + »	More specific type/id for the event	[Noted as incomplete, no definitions – 23 Sep 2014] Read Vread Update Delete Validate Create History-instance History-type History-system Search-type Search-system Transaction + DICOM codeset	
action : code 0..1 « SecurityEventAction »	Type of action performed during the event	C) Create R) Read/view/print U) Update D) Delete E) Execute.	
reason : CodeableConcept 0..1	Reason activity is occurring	[None]	TBD
Resource – SecurityEvent.Source 1..1 – Application systems and processes			
type : CodeableConcept 1..1 « SecurityEventSourceType+ »	The type of source where event originated	[Noted as incomplete – 23 Sep 2014] 1) User Device: End-user display device, diagnostic device 2) Data Interface: Data acquisition device or instrument 3) Web Server: Web server process or thread 4) Application Server: Application server process or thread 5) Database Server: Database server process or thread 6) Security Server: Security server, e.g., a domain controller 7) Network Device: ISO level 1-3 network component 8) Network Router: ISO level 4-6 operating software 9) Other: Other kind of device (defined by DICOM or other code)	

Resource Attribute	Description	Code/Value: Description	Notes or Proposal
Resource – SecurityEvent.Object 0..* – Specific instances of data or objects accessed			
type : code 0..1 « SecurityEventObjectType »	Object type being audited	1) Person 2) System Object 3) Organization 4) Other.	
role : code 0..1 « SecurityEventObjectRole »	Functional application role of Object	1) Patient: This object is the patient that is the subject of care related to this event. It is identifiable by patient ID or equivalent. The patient may be either human or animal. 2) Location: This is a location identified as related to the event. This is usually the location where the event took place. Note that for shipping, the usual events are arrival at a location or departure from a location. 3) Report: This object is any kind of persistent document created as a result of the event. This could be a paper report, film, electronic report, DICOM Study, etc. Issues related to medical records life cycle management are conveyed elsewhere. 4) Resource: A logical object related to the event. (Deprecated). 5) Master file: This is any configurable file used to control creation of documents. Examples include the objects maintained by the HL7 Master File transactions, Value Sets, etc. 6) User: A human participant not otherwise identified by some other category 7) List: (deprecated). 8) Doctor: Typically a licensed person who is providing or performing care related to the event, generally a physician. The key distinction between doctor and practitioner is with regards to their role, not the licensing. The doctor is the human who actually performed the work. The practitioner is the human or organization that is responsible for the work. 9) Subscriber: A person or system that is being notified as part of the event. This is relevant in situations where automated systems provide notifications to other parties when an event took place. 10) Guarantor: Insurance company, or any other organization who accepts responsibility for paying for the healthcare event. 11) Security user entity: A person or active system object involved in the event with a security role. 12) Security user group: A person or system object involved in the event with the authority to modify security roles of other objects. 13) Security resource: A passive object, such as a role table, that is relevant to the event. 14) Security granularity definition: (deprecated) Relevant to certain RBAC security methodologies. 15) Practitioner: Any person or organization responsible for providing care. This encompasses all forms of care, licensed or otherwise, and all sorts of teams and care groups. Note, the distinction between practitioners and the doctor that actually provided the care to the patient. 16) Data destination: The source or destination for data transfer, when it does not match some other role.	

		17) Data repository: A source or destination for data transfer, that acts as an archive, database, or similar role. 18) Schedule: An object that holds schedule information. This could be an appointment book, availability information, etc. 19) Customer: An organization or person that is the recipient of services. This could be an organization that is buying services for a patient, or a person that is buying services for an animal. 20) Job: An order, task, work item, procedure step, or other description of work to be performed. E.g., a particular instance of an MPPS. 21) Job stream: A list of jobs or a system that provides lists of jobs. E.g., an MWL SCP. 22) Table: (deprecated) 23) Routing criteria: An object that specifies or controls the routing or delivery of items. For example, a distribution list is the routing criteria for mail. The items delivered may be documents, jobs, or other objects. 24) Query: The contents of a query. This is used to capture the contents of any kind of query. For security surveillance purposes knowing the queries being made is very important.	
lifecycle : code 0..1 « SecurityEventObjectLifecycle »	Life-cycle stage for the object	1) Origination/Creation 2) Import/Copy from original 3) Amendment 4) Verification 5) Translation 6) Access/Use 7) De-identification 8) Aggregation, summarization, derivation 9) Report 10) Export/Copy to target 11) Disclosure 12) Receipt of disclosure 13) Archiving 14) Logical deletion 15) Permanent erasure/Physical destruction	[From EHR-S FM R2:] 1) Originate/retain 2) Amend/update 3) Translate 4) Attest 5) View/Access 6) Output/Report 7) Disclose 8) Transmit 9) Receive/Retain 10) De-Identify 11) Pseudonymize 12) Re-Identify 13) Extract 14) Archive 15) Restore 16) Destroy/Delete 17) Deprecate/Retract 18) Re-Activate 19) Merge 20) Unmerge 21) Link 22) Unlink 23) Place Legal Hold 24) Remove Legal Hold 25) Verify 26) Encrypt 27) Decrypt

sensitivity : code 0..1 «SecurityEventObject.sensitivity »	Policy-defined sensitivity for the object	**L) Low**: Privacy metadata indicating that the information has been de-identified, and there are mitigating circumstances that prevent re-identification, which minimize risk of harm from unauthorized disclosure. The information requires protection to maintain low sensitivity. > Examples: Includes anonymized, pseudonymized, or non-personally identifiable information such as HIPAA limited data sets. > Map: No clear map to ISO 13606-4 Sensitivity Level (1) Care Management: RECORD_COMPONENTs that might need to be accessed by a wide range of administrative staff to manage the subject of care's access to health services. > Usage Note: This metadata indicates the receiver may have an obligation to comply with a data use agreement. **M) Moderate**: Privacy metadata indicating moderately sensitive information, which presents moderate risk of harm if disclosed without authorization. > Examples: Includes allergies of non-sensitive nature used inform food service; health information a patient authorizes to be used for marketing, released to a bank for a health credit card or savings account; or information in personal health record systems that are not governed under health privacy laws. > Map: Partial Map to ISO 13606-4 Sensitivity Level (2) Clinical Management: Less sensitive RECORD_COMPONENTs that might need to be accessed by a wider range of personnel not all of whom are actively caring for the patient (e.g. radiology staff). > Usage Note: This metadata indicates that the receiver may be obligated to comply with the receiver's terms of use or privacy policies. **N) Normal**: Privacy metadata indicating that the information is typical, non-stigmatizing health information, which presents typical risk of harm if disclosed without authorization. > Examples: In the US, this includes what HIPAA identifies as the minimum necessary protected health information (PHI) given a covered purpose of use (treatment, payment, or operations). Includes typical, non-stigmatizing health information disclosed in an application for health, workers compensation, disability, or life insurance. > Map: Partial Map to ISO 13606-4 Sensitivity Level (3) Clinical Care: Default for normal clinical care access (i.e. most clinical staff directly caring for the patient should be able to access nearly all of the EHR). Maps to normal confidentiality for treatment information but not to ancillary care, payment and operations. > Usage Note: This metadata indicates that the receiver may be obligated to comply with applicable jurisdictional privacy law or disclosure authorization. **R) Restricted**: Privacy metadata indicating highly sensitive, potentially stigmatizing information, which presents a high risk to the information subject if disclosed without authorization. May be preempted by jurisdictional law, e.g., for public health reporting or emergency treatment. > Examples: In the US, this includes what HIPAA identifies as the minimum necessary protected health information (PHI) given a covered purpose of use (treatment, payment, or operations). Includes typical, non-stigmatizing health information disclosed in an application for health, workers compensation, disability, or life insurance. > Map: Partial Map to ISO 13606-4 Sensitivity Level (3) Clinical Care: Default for normal clinical care access (i.e. most clinical staff directly caring for the patient	

		should be able to access nearly all of the EHR). Maps to normal confidentiality for treatment information but not to ancillary care, payment and operations. > Usage Note: This metadata indicates that the receiver may be obligated to comply with applicable, prevailing (default) jurisdictional privacy law or disclosure authorization. **U) Unrestricted**: Privacy metadata indicating that the information is not classified as sensitive. > Examples: Includes publicly available information, e.g., business name, phone, email or physical address. > Usage Note: This metadata indicates that the receiver has no obligation to consider additional policies when making access control decisions. Note that in some jurisdictions, personally identifiable information must be protected as confidential, so it would not be appropriate to assign a confidentiality code of "unrestricted" to that information even if it is publicly available. **V) Very restricted**: Privacy metadata indicating that the information is extremely sensitive and likely stigmatizing health information that presents a very high risk if disclosed without authorization. This information must be kept in the highest confidence. > Examples: Includes information about a victim of abuse, patient requested information sensitivity, and taboo subjects relating to health status that must be discussed with the patient by an attending provider before sharing with the patient. May also include information held under “legal lock” or attorney-client privilege > Map: This metadata indicates that the receiver may not disclose this information except as directed by the information custodian, who may be the information subject. > Usage Note: This metadata indicates that the receiver may not disclose this information except as directed by the information custodian, who may be the information subject.	
Resource – SecurityEvent.Participant 1..* – A person, a hardware device or software process			
role : CodeableConcept 0..* « DICOMRoleId+ »	User roles (e.g. local RBAC codes)	[As listed – 23 September 2014] 110150 110151 110152 110153 110154 110155	
Resource – SecurityEvent.Participant.Network 0..1 – Logical network location for application activity			
type : code 0..1 « SecurityEventParticipantNetworkType »	The type of network access point	1 Machine Name, including DNS name. 2 IP Address. 3 Telephone Number. 4 Email address. 5 URI (User directory, HTTP-PUT, ftp, etc.).	