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 – 11 November 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	[See Purpose of Use table at the end of this document]	
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	[Noted as incomplete] 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	[Noted as incomplete] 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	[Noted as incomplete] Rest + DICOM codeset as follows: 110100 – Application Activity – Audit event: Application Activity has taken place 110101 – Audit Log Used – Audit event: Audit Log has been used 110102 – Begin Transferring DICOM Instances – Audit event: Storage of DICOM Instances has begun 110103 – DICOM Instances Accessed – Audit event: DICOM Instances have been created, read, updated, or deleted 110104 – DICOM Instances Transferred – Audit event: Storage of DICOM Instances has been completed 110105 – DICOM Study Deleted – Audit event: Entire Study has been deleted 110106 – Export – Audit event: Data has been exported out of the system 110107 – Import – Audit event: Data has been imported into the system 110108 – Network Entry – Audit event: System has joined or left network 110112 – Query – Audit event: Query has been made 110113 – Security Alert – Audit event: Security Alert has been raised 110114 – User Authentication – Audit event: User Authentication has been attempted	
subtype : CodeableConcept 0..* « SecurityEventSubType + »	More specific type/id for the event	[Noted as incomplete] Read Vread Update Delete Validate Create History-instance History-type History-system Search-type Search-system Transaction + DICOM codeset as follows: 110120 – Application Start – Audit event: Application Entity has started 110121 – Application Stop – Audit event: Application Entity has stopped 110122 – Login – Audit event: User login has been attempted 110123 – Logout – Audit event: User logout has been attempted 110124 – Attach – Audit event: Node has been attached 110125 – Detach – Audit event: Node has been detached 110126 – Node Authentication – Audit event: Node Authentication has been attempted 110127 – Emergency Override Started – Audit event: Emergency Override has started 110128 – Network Configuration – Audit event: Network configuration has been changed 110129 – Security Configuration – Audit event: Security configuration has been changed 110130 – Hardware Configuration – Audit event: Hardware configuration has been changed 110131 – Software Configuration – Audit event: Software configuration has been changed 110132 – Use of Restricted Function – Audit event: A use of a restricted function has been attempted 110133 – Audit Recording Stopped – Audit event: Audit recording has been stopped 110134 – Audit Recording Started – Audit event: Audit recording has been started	

		110135 – Object Security Attributes Changed – Audit event: Security attributes of an object have been changed 110136 – Security Roles Changed – Audit event: Security roles have been changed 110137 – User security Attributes Changed – Audit event: Security attributes of a user have been changed 110138 – Emergency Override Stopped – Audit event: Emergency Override has Stopped 110139 – Remote Service Operation Started – Audit event: Remote Service Operation has Begun 110140 – Remote Service Operation Stopped – Audit event: Remote Service Operation has Stopped 110141 – Local Service Operation Started – Audit event: Local Service Operation has Begun 110142 – Local Service Operation Stopped – Audit event: Local Service Operation Stopped	
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	[See Purpose of Use table at the end of this document]	
Resource – SecurityEvent.Source 1..1 – Application systems and processes			
type : CodeableConcept 1..1 « SecurityEventSourceType+ »	The type of source where event originated	[Noted as incomplete] 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)	[Noted as incomplete] DICOM codeset as follows: 110150 – Application – Audit participant role ID of software application 110151 – Application Launcher – Audit participant role ID of software application launcher, i.e., the entity that started or stopped an application. 110152 – Destination Role ID – Audit participant role ID of the receiver of data 110153 – Source Role ID – Audit participant role ID of the sender of data 110154 – Destination Media – Audit participant role ID of media receiving data during an export. 110155 – Source Media – Audit participant role ID of media providing data during an import.	
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.).	

Purpose of Use **C:ActReason:PurposeOfUse:23408** **V:PurposeOfUse:2.16.840.1.113883.1.11.20448** **V:GeneralPurposeOfUse:2.16.840.1.113883.1.11.20449**			
Lvl- Typ	**Concept Code** ***Head Code-defined Value Set***	**Print Name**	**Definition, Properties, Relationships**
For XSPA – use General Purpose of Use value set, which is the subset of the POU codes below in tan colored rows.			
2-**A**	**PurposeOfUse** v:PurposeOfUse; v:GeneralPurposeOfUse	purpose of use	**Definition:** Reason for performing one or more operations on information, which may be permitted by source system's security policy in accordance with one or more privacy policies and consent directives. Description: The rationale or purpose for an act relating to the management of personal health information, such as collecting personal health information for research or public health purposes. **Concept Relationships:** **Specializes:** _ActHealthInformationManagementReason **Generalizes (derived):** TREAT HPAYMT HOPERAT HMARKT HRESCH PATRQT
3-**S**	**HMARKT**	healthcare marketing	**Definition:** To perform one or more operations on information for marketing services and products related to health care.
3-**S**	**HOPERAT**	healthcare operations	**Definition:** To perform one or more operations on information used for conducting administrative and contractual activities related to the provision of health care. **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** DONAT FRAUD GOV HACCRED HCOMPL HDECD HDIRECT HLEGAL HOUTCOMS HPRGRP HQUALIMP HSYSADMIN MEMADMIN PATADMIN PATSFTY PERFMSR RECORDMGT TRAIN
4-**L**	**DONAT**	donation	**Definition:** To perform one or more operations on information used for cadaveric organ, eye or tissue donation.
4-**L**	**FRAUD**	fraud	**Definition:** To perform one or more operations on information used for fraud detection and prevention processes.
4-**L**	**GOV**	government	**Definition:** To perform one or more operations on information used within government processes.
4-**L**	**HACCRED**	accreditation	**Definition:** To perform one or more operations on information for conducting activities related to meeting accreditation criteria.
4-**L**	**HCOMPL**	compliance	**Definition:** To perform one or more operations on information used for conducting activities required to meet a mandate.
4-**L**	**HDECD**	decedent	**Definition:** To perform one or more operations on information used for handling deceased patient matters.
4-**L**	**HDIRECT**	directory	**Definition:** To perform one or more operation operations on information used to manage a patient directory. Examples: Facility, enterprise, payer, or health information exchange patient directory.

4-**L**	**HLEGAL**	legal	**Definition:** To perform one or more operations on information for conducting activities required by legal proceeding.
4-**L**	**HOUTCOMS**	outcome measure	**Definition:** To perform one or more operations on information used for assessing results and comparative effectiveness achieved by health care practices and interventions.
4-**L**	**HPRGRP**	program reporting	**Definition:** To perform one or more operations on information used for conducting activities to meet program accounting requirements.
4-**L**	**HQUALIMP**	quality improvement	**Definition:** To perform one or more operations on information used for conducting administrative activities to improve health care quality.
4-**L**	**HSYSADMIN**	system administration	**Definition:** To perform one or more operations on information to administer the electronic systems used for the delivery of health care.
4-**L**	**MEMADMIN**	member administration	**Definition:** To perform one or more operations on information to administer health care coverage to an enrollee under a policy or program.
4-**L**	**PATADMIN**	patient administration	**Definition:** To perform one or more operations on information used for operational activities conducted to administer the delivery of health care to a patient.
4-**L**	**PATSFTY**	patient safety	**Definition:** To perform one or more operations on information in processes related to ensuring the safety of health care.
4-**L**	**PERFMSR**	performance measure	**Definition:** To perform one or more operations on information used for monitoring performance of recommended health care practices and interventions.
4-**L**	**RECORDMGT**	records management	**Definition:** To perform one or more operations on information used within the health records management process.
4-**L**	**TRAIN**	training	**Definition:** To perform one or more operations on information used in training and education.
3-**S**	**HPAYMT**	healthcare payment	**Definition:** To perform one or more operations on information for conducting financial or contractual activities related to payment for provision of health care. **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** ELIGDTRM CLMATTCH COVAUTH REMITADV
4-**L**	**COVERAGE**	coverage under policy or program	**Definition:** To perform one or more operations on information for conducting activities related to coverage under a program or policy.
5-**L**	**ELIGDTRM**	eligibility determination	**Definition:** To perform one or more operations on information used for conducting eligibility determination for coverage in a program or policy. May entail review of financial status or disability assessment.
5-**L**	. . . . . **ELIGVER**	eligibility verification	**Definition:** To perform one or more operations on information used for conducting eligibility verification of coverage in a program or policy. May entail provider contacting coverage source (e.g., government health program such as workers compensation or health plan) for confirmation of enrollment, eligibility for specific services, and any applicable copays.
5-**L**	**ENROLLM**	enrollment	**Definition:** To perform one or more operations on information used for enrolling a covered party in a program or policy. May entail recording of covered party's and any dependent's demographic information and benefit choices.

4-**L**	**CLMATTCH**	claim attachment	**Definition:** To perform one or more operations on information for provision of additional clinical evidence in support of a request for coverage or payment for health services.
4-**L**	**COVAUTH**	coverage authorization	**Definition:** To perform one or more operations on information for conducting prior authorization or predetermination of coverage for services.
4-**L**	**REMITADV**	remittance advice	**Definition:** To perform one or more operations on information about the amount remitted for a health care claim.
3-**S**	**HRESCH**	healthcare research	**Definition:** To perform one or more operations on information for conducting scientific investigations to obtain health care knowledge. **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** CLINTRCH
4-**L**	**CLINTRCH**	clinical trial research	**Definition:** To perform one or more operations on information for conducting scientific investigations in accordance with clinical trial protocols to obtain health care knowledge.
3-**S**	**PATRQT**	patient requested	**Definition:** To perform one or more operations on information in response to a patient's request. **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** FAMRQT PWATRNY SUPNWK
4-**L**	**FAMRQT**	family requested	**Definition:** To perform one or more operations on information in response to a request by a family member authorized by the patient.
4-**L**	**PWATRNY**	power of attorney	**Definition:** To perform one or more operations on information in response to a request by a person appointed as the patient's legal representative.
4-**L**	**SUPNWK**	support network	**Definition:** To perform one or more operations on information in response to a request by a person authorized by the patient.
3-**S**	**PUBHLTH**		**Definition:** To perform one or more operations on information for conducting public health activities, such as the reporting of notifiable conditions. **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** DISASTER THREAT
4-**L**	**DISASTER**		**Definition:** To perform one or more operations on information used for provision of immediately needed health care to a population of living subjects located in a disaster zone.
4-**L**	**THREAT**		**Definition:** To perform one or more operations on information used to prevent injury or disease to living subjects who may be the target of violence.
3-**S**	**TREAT**	treatment	**Definition:** To perform one or more operations on information for provision of health care. **Concept Relationships:** **Specializes:** PurposeOfUse **Generalizes (derived):** CAREMGT CLINTRL ETREAT POPHLTH
4-**L**	**CAREMGT**	care management treatment	**Definition:** To perform one or more operations on information for provision of health care coordination.

4-**L**	**CLINTRL**	clinical trial treatment	**Definition:** To perform one or more operations on information for provision of health care within a clinical trial.
4-**L**	**ETREAT**	emergency treatment	**Definition:** To perform one or more operations on information for provision of immediately needed health care for an emergent condition.
4-**L**	**POPHLTH**	population health treatment	**Definition:** To perform one or more operations on information for provision of health care to a population of living subjects, e.g., needle exchange program.