SecurityEvent Fhir Resource Proposal
Contents

• 1 SecurityEvent
  • 1.1 Owning committee name
  • 1.2 Contributing or Reviewing Work Groups
  • 1.3 FHIR Resource Development Project Insight ID
  • 1.4 Scope of coverage
  • 1.5 RIM scope
  • 1.6 Resource appropriateness
  • 1.7 Expected implementations
  • 1.8 Content sources
  • 1.9 Example Scenarios
  • 1.10 Resource Relationships
  • 1.11 Timelines
  • 1.12 gForge Users
SecurityEvent

Owning committee name
IHE IT Infrastructure Technical Committee

Contributing or Reviewing Work Groups
- Security
- EHR
- Community-Based Collaborative Care

FHIR Resource Development Project Insight ID
unclear how to reference external organization ownership

Scope of coverage
User Accountability is provided through a Security Audit Trail. The Audit Trail needs to allow a Security officer in an institution to audit activities, to assess compliance with a secure domain’s policies, to detect instances of non-compliant behavior, and to facilitate detection of improper creation, access, modification and deletion of Protected Health Information (PHI). The Audit Trail should provide Privacy officer in an institution to audit privacy compliance, and aid in the production of an Accounting of Disclosures.

The Audit Trail needs to contain sufficient record of security and privacy relevant events. The Audit Trail is a protected resource, but should contain minimal unnecessary exposure leveraging persistent opaque identifiers when ever possible. Audit Trail Reporting should leverage Directories, Registries, and other databases to resolve opaque identifiers as necessary. Reporting is an auditable event.

RIM scope
Security and Privacy are different domains from the RIM. The overlap with the RIM is not necessary, but to be leveraged when appropriate.

Resource appropriateness
- Leverages well established Security and Privacy concepts

Expected implementations
- USA - Regulations from HHS/ONC/CMS looking for RESTful implementations of IHE-ATNA Audit Logging
- Others have expressed interest in RESTful implementations of IHE-ATNA Audit Logging

Content sources
- ASTM E2147: Setup the concept of security audit logs for healthcare including accounting of disclosures
- IETF RFC 3881: Defined the Information Model (IETF rule forced this to be informative)
- DICOM Audit Log Message: Made the information model Normative, defined Vocabulary, Transport Binding, and Schema
- IHE ATNA: defines the grouping with secure transport and access controls; and defined specific audit log records for specific IHE transactions.
- NIST SP800-92: shows how to do audit log management and reporting consistent with our model
- HL7 PASS: Defined an Audit Service with responsibilities and a query interface for reporting use
- ISO 27789: is defining the subset of audit events that an EHR would need

Example Scenarios
- Record a Security relevant event has happened - Login, Logout, System Start, Patient information viewed, Patient Information exported
- Record a Privacy relevant event has happened – A Disclosure
- Security Officer needs to look for abuse of security policies
  - too many failed login events indicate a potential attack
  - Review accesses by a specific user
  - Review accesses to a specific patient
  - Review inappropriate access from a workstation
  - Review inappropriate access from a region/department
- Privacy Officer needs to
  - Produce an Accounting of Disclosures for a specific Patient
  - Produce an Access Log for a specific Patient
  - Produce a Disclosure report on a population
  - Review an accusation of inappropriate access
Resource Relationships

none directly. Many references should be made to this Resource through Security Considerations

Timelines

Interest in this resource for use by reporting tools

gForge Users

john_moehrke