HL7 AUSTRIA

Security & FHIR

FH-Prof. DI Alexander Mense
FH Technikum Wien

Wien, 18.5.2022

A world in which everyone can securely access and use the right health data when and where they need it.

HL7 Vision

Security on FHIR – don‘t get burned!

- Alissa Knight

https://approov.io/

General approach

- “FHIR is not a security protocol, nor does it define any security related functionality. However, FHIR does define exchange protocols and content models that need to be used with various security protocols defined elsewhere.”

- “FHIR does not mandate a single technical approach to security and privacy; rather, the specification provides a set of building blocks that can be applied to create secure, private systems.”

Was bedeutet das?

- FHIR beschreibt weder grundlegende Security Anforderungen (sind abhängig von spezifischen Policies) noch spezifische Technologien für die Implementierung
- Jeder Implementer ist selbst verantwortlich, dass zum Beispiel …
  - Die Kommunikation verschlüsselt und authentifiziert erfolgt
    - Z.B. Einsatz von TLS
  - Im Fehlerfall keine sensitive Information geleakt wird
  - Best practices für Applikationsicherheit angewandt werden
    - Input validation
    - Verhindern von Script Injections beim .text Element von Ressourcen (narrative)
    - Keine Credentials im Code
  - Audit Trails verfügbar sind
  - Access Control korrekt umgesetzt wird
- Welche Art der Authentifizierung, Access Control und Protokollierung hängt von der jeweiligen Policy ab

Beispiel

- Use case: "A FHIR server should keep a complete, tamper-proof log of all API access and other security- and privacy-relevant events".
- Approach: FHIR provides an AuditEvent resource suitable for use by FHIR clients and servers to record when a security or privacy relevant event has occurred.
  This form of audit logging records as much detail as reasonable at the time the event happened. The FHIR AuditEvent is aligned and cross-referenced with IHE Audit Trail and Node Authentication (ATNA) Profile.
- https://www.hl7.org/fhir/secpriv-module.html

Security & Privacy Building blocks

- Resources
  - AuditEvent (http://hl7.org/fhir/auditevent.html)
  - Consent (http://hl7.org/fhir/consent.html)
  - Provenance (http://hl7.org/fhir/provenance.html)
- Data Types
  - Digital Signature (http://hl7.org/fhir/datatypes.html#signature)
- Implementation Guidance and Principles
  - Security Principles (http://hl7.org/fhir/security.html)
  - Security Labels (http://hl7.org/fhir/security-labels.html)
  - Signatures (http://hl7.org/fhir/signatures.html)
  - Access Control (z.B. Smart on FHIR)

AuditEvent

- Zur Aufzeichnung von Systemevents um in der Regel ein Security Log umsetzen
- Zur Überwachung von Security (und Privacy) relevanten Ereignissen
  - user login and logout, access control decisions, configuration events, …
- based on the IHE-ATNA Audit record definitions, originally from RFC 3881, and now managed by DICOM
- Akteure wie Applikationen, Prozesse oder Services, die in sogenannte “auditable events” involviert sind, sollen AuditEvents aufzeichnen
- Siehe auch brand-new IHE BALP Profil (https://profiles.ihe.net/ITI/BALP/index.html)

AuditEvent

Structure

Name	Flags	Card.	Type	Description & Constraints
AuditEvent	TU		DomainResource	Event record kept for security purposes Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
type	Σ	1..1	Coding	Type/identifier of event Audit Event ID (Extensible)
subtype	Σ	0..*	Coding	More specific type/id for the event Audit Event Sub-Type (Extensible)
action	Σ	0..1	code	Type of action performed during the event AuditEventAction (Required)
period		0..1	Period	When the activity occurred
recorded	Σ	1..1	instant	Time when the event was recorded
outcome	Σ	0..1	code	Whether the event succeeded or failed AuditEventOutcome (Required)
outcomeDesc	Σ	0..1	string	Description of the event outcome
purposeOfEvent	Σ	0..*	CodeableConcept	The purposeOfUse of the event V3 Value SetPurposeOfUse (Extensible)
agent		1..*	BackboneElement	Actor involved in the event
type		0..1	CodeableConcept	How agent participated ParticipationRoleType (Extensible)
role		0..*	CodeableConcept	Agent role in the event SecurityRoleType (Example)
who	Σ	0..1	Reference(PractitionerRole | Practitioner | Organization | Device | Patient | RelatedPerson)	Identifier of who
altId		0..1	string	Alternative User identity
name		0..1	string	Human friendly name for the agent

AuditEvent.type (extensible)

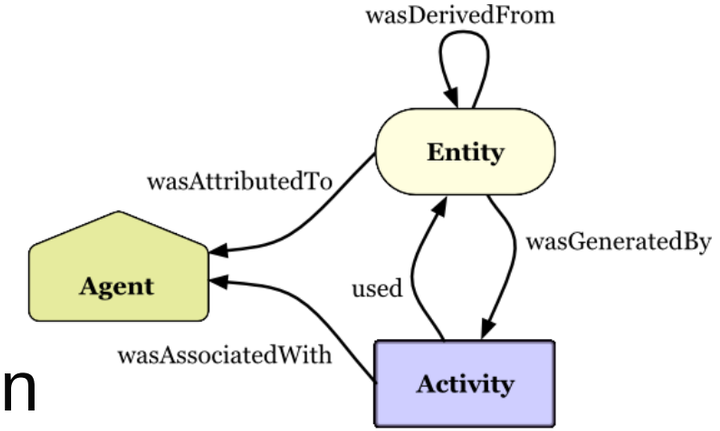
Code	Display	
110100	Application Activity	Audit event: Application Activity has taken place
110101	Audit Log Used	Audit event: Audit Log has been used
110102	Begin Transferring DICOM Instances	Audit event: Storage of DICOM Instances has begun
110103	DICOM Instances Accessed	Audit event: DICOM Instances have been created, read, upda
110104	DICOM Instances Transferred	Audit event: Storage of DICOM Instances has been complete
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
110109	Order Record	Audit event: Order has been created, read, updated or delete
110110	Patient Record	Audit event: Patient Record has been created, read, updated
110111	Procedure Record	Audit event: Procedure Record has been created, read, updat
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

AuditEvent.subtype (extensible)

Code	Display	
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

Provenance

- Provencance enthält Informationen über Aktivitäten betreffend Erzeugen, verändern, löschen, Signieren einer Version einer Resource und beschreibt Entitäten und beteiligte Agends
- Essentiell für
  - Authentizität
  - Nachvollziehbarkeit
  - Reliability
  - Integrität
  - Vertrauen
- Basiert auf der W3C Provence Specification
- Signieren einer Resource resuliert in einem Provenance Record mit der digitalen Unterschrift
- Provenance deckt Erzeugen/Verändern von Resourcen ab, wohingegen AuditEvent die Verwendung abbildet



Provenance

Name	Flags	Card.	Type	Description & Constraints
Provenance	TU		DomainResource	Who, What, When for a set of resources Elements defined in Ancestors: id, meta, implicitRules, language, text, contained, extension, modifierExtension
target	Σ	1..*	Reference(Any)	Target Reference(s) (usually version specific)
occurred[x]		0..1		When the activity occurred
occurredPeriod			Period	
occurredDateTime			dateTime	
recorded	Σ	1..1	instant	When the activity was recorded / updated
policy		0..*	uri	Policy or plan the activity was defined by
location		0..1	Reference(Location)	Where the activity occurred, if relevant
reason		0..*	CodeableConcept	Reason the activity is occurring V3 Value SetPurposeOfUse (Extensible)
activity		0..1	CodeableConcept	Activity that occurred Provenance activity type (Extensible)
agent		1..*	BackboneElement	Actor involved
type	Σ	0..1	CodeableConcept	How the agent participated Provenance participant type (Extensible)
role		0..*	CodeableConcept	What the agents role was SecurityRoleType (Example)
who	Σ	1..1	Reference(Practitioner | PractitionerRole | RelatedPerson | Patient | Device | Organization)	Who participated
onBehalfOf		0..1	Reference(Practitioner | PractitionerRole | RelatedPerson | Patient | Device | Organization)	Who the agent is representing
entity		0..*	BackboneElement	An entity used in this activity
role	Σ	1..1	code	derivation | revision | quotation | source | removal ProvenanceEntityRole (Required)
what	Σ	1..1	Reference(Any)	Identity of entity
agent		0..*	see agent	Entity is attributed to this agent
signature		0..*	Signature	Signature on target

Consent

- Resource um einen Consent im medizinischen Kontext auszudrücken
- Healthcare Consumer
  - Gibt Erlaubnis oder verbietet …
  - Einer Person, Organisation oder Rolle
  - Eine oder mehrere Aktionen zu setzen (access, share, …)
  - in einem gegebenen Policy Kontext
  - Für einen bestimmten Purpose of Use
  - Für eine bestimmte Zeit
- Anwendung in einem von vier Bereichen
  - Privacy Consent Directive: Agreement to collect, access, use or disclose (share) information.
  - Medical Treatment Consent Directive: Consent to undergo a specific treatment (or record of refusal to consent).
  - Research Consent Directive: Consent to participate in research protocol and information sharing required.
  - Advance Care Directives: Consent to instructions for potentially needed medical treatment (e.g. DNR).
- Im Moment nur Privacy Consent modelliert

Consent

Name	Flags	Card.	Type	Description & Constraints
Consent	I TU		DomainResource	A healthcare consumer's choices to permit or deny recipients or periods of time *+ Rule: Either a Policy or PolicyRule* *+ Rule: IF Scope=privacy, there must be a patient* *+ Rule: IF Scope=research, there must be a patient* *+ Rule: IF Scope=adr, there must be a patient* *+ Rule: IF Scope=treatment, there must be a patient* Elements defined in Ancestors: id, meta, implicitRules, languag
identifier	Σ	0..*	Identifier	Identifier for this record (external references)
status	?! Σ	1..1	code	draft | proposed | active | rejected | inactive | entered-in-error ConsentState (Required)
scope	?! Σ	1..1	CodeableConcept	Which of the four areas this resource covers (extensible) Consent Scope Codes (Extensible)
category	Σ	1..*	CodeableConcept	Classification of the consent statement - for indexing/retrieval Consent Category Codes (Extensible)
patient	Σ	0..1	Reference(Patient)	Who the consent applies to
dateTime	Σ	0..1	dateTime	When this Consent was created or indexed
performer	Σ	0..*	Reference(Organization | Patient | Practitioner | RelatedPerson | PractitionerRole)	Who is agreeing to the policy and rules
organization	Σ	0..*	Reference(Organization)	Custodian of the consent
source[x]	Σ	0..1		Source from which this consent is taken
sourceAttachment			Attachment	
sourceReference			Reference(Consent | DocumentReference | Contract | QuestionnaireResponse)	
policy		0..*	BackboneElement	Policies covered by this consent
authority	I	0..1	uri	Enforcement source for policy
uri	I	0..1	uri	Specific policy covered by this consent
policyRule	Σ I	0..1	CodeableConcept	Regulation that this consents to Consent PolicyRule Codes (Extensible)
verification	Σ	0..*	BackboneElement	Consent Verified by patient or family
verified	Σ	1..1	boolean	Has been verified
verifiedWith		0..1	Reference(Patient | RelatedPerson)	Person who verified
verificationDate		0..1	dateTime	When consent verified
provision	Σ	0..1	BackboneElement	Constraints to the base Consent.policyRule
type	Σ	0..1	code	deny | permit ConsentProvisionType (Required)
period	Σ	0..1	Period	Timeframe for this rule
actor		0..*	BackboneElement	Who|what controlled by this rule (or group, by role)
role		1..1	CodeableConcept	How the actor is involved SecurityRoleType (Extensible)
reference		1..1	Reference(Device |	Resource for the actor (or group, by role)


```
{
  "resourceType": "Consent",
  "id": "consent-example-basic",
  "text": {
    "status": "generated",
    "div": "<div xmlns=\"http://www.w3.org/1999/xhtml\">\n\t\t\t<p>\n\tAuthorize Normal access f
or Treatment\n\t\t\t</p>\n\t\t\t<p>\n    Patient &quot;P. van de Heuvel&quot; wishes to have all
of the PHI collected at the Good Health Psychiatric Hospital \n   available for normal treatment
use.\n\t\t\t</p>\n\t\t</div>"
  },
  "status": "active",
  "scope": {
    "coding": [
      {
        "system": "http://terminology.hl7.org/CodeSystem/consentscope",
        "code": "patient-privacy"
      }
    ]
  },
  "category": [
    {
      "coding": [
        {
          "system": "http://loinc.org",
          "code": "59284-0"
        }
      ]
    }
  ],
  "patient": {
    "reference": "Patient/f001",
    "display": "P. van de Heuvel"
  },
  "dateTime": "2016-05-11",
  "organization": [
    {
      "reference": "Organization/f001"
    }
  ],
  "sourceAttachment": {
    "title": "The terms of the consent in lawyer speak."
  },
  "policyRule": {
    "coding": [
      {
        "system": "http://terminology.hl7.org/CodeSystem/v3-ActCode",
        "code": "OPTIN"
      }
    ]
  },
  "provision": {
    "period": {
      "start": "1964-01-01",
      "end": "2016-01-01"
    }
  }
```

Consent.policyRule

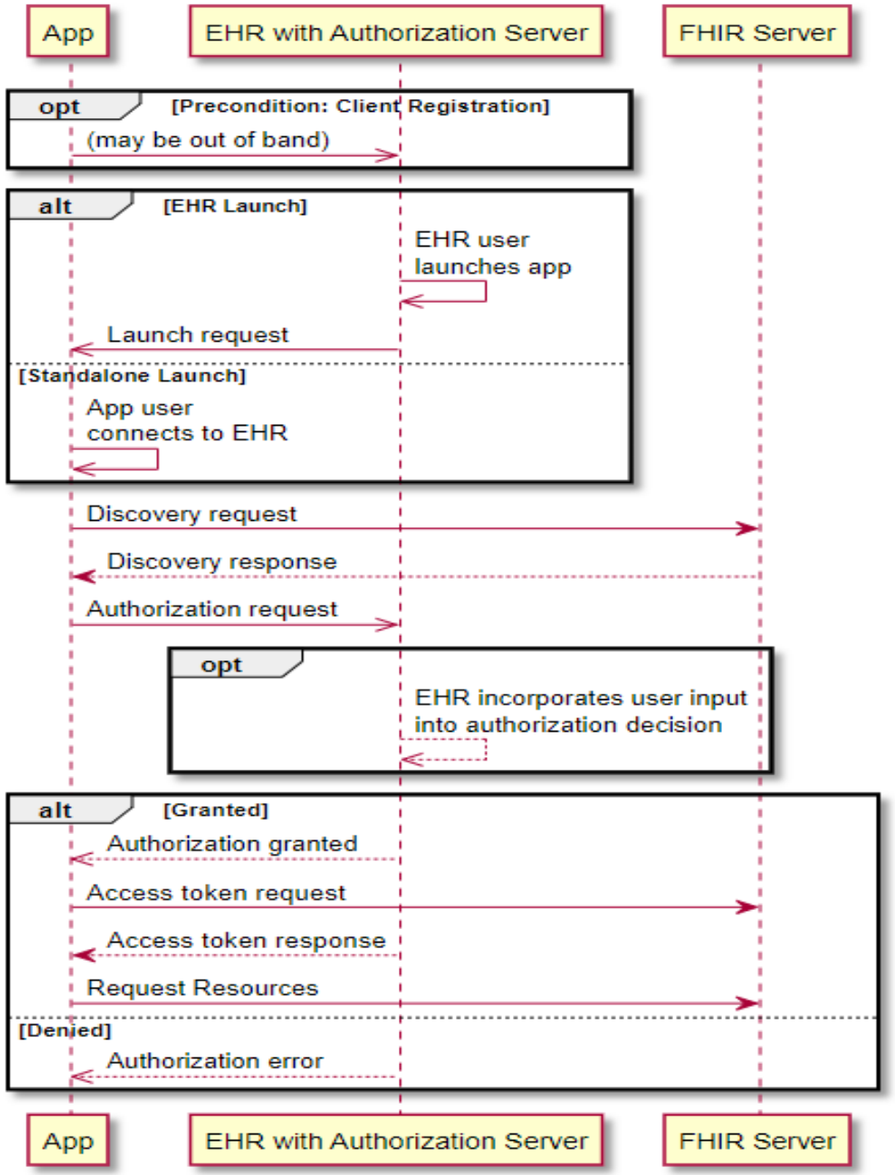
	HIPAA consent	
nl-lsp	NL LSP Permission	LSP (National Exchange Point) requires that providers, hospitals and pharmacy obtain explicit permission [opt-in] from healthcare consumers to submit and retrieve all or only some of a subject of care's health information collected by the LSP for purpose of treatment, which can be revoked. Without permission, a provider cannot access LSP information even in an emergency. The LSP provides healthcare consumers with accountings of disclosures. https://www.vzvz.nl/uploaded/FILES/htmlcontent/Formulieren/TOESTEMMINGSFORMULIER.pdf, https://www.ikgeeftoestemming.nl/en, https://www.ikgeeftoestemming.nl/en/registration/find-healthcare-provider
at-elga	AT ELGA Opt-in Consent	Pursuant to Sec. 2 no. 9 Health Telematics Act 2012, ELGA Health Data ("ELGA-Gesundheitsdaten") = Medical documents. Austria opted for an opt-out approach. This means that a person is by default 'ELGA participant' unless he/she objects. ELGA participants have the following options: General opt out: No participation in ELGA, Partial opt-out: No participation in a particular ELGA application, e.g. eMedication and Case-specific opt-out: No participation in ELGA only regarding a particular case/treatment. There is the possibility to opt-in again. ELGA participants can also exclude the access of a particular ELGA healthcare provider to a particular piece of or all of their ELGA data. http://ec.europa.eu/health/ehealth/docs/laws_austria_en.pdf
nih-hipaa	HHS NIH HIPAA Research Authorization	Guidance and template form https://privacyruleandresearch.nih.gov/pdf/authorization.pdf
nci	NCI Cancer Clinical Trial consent	see http://ctep.cancer.gov/protocolDevelopment/docs/Informed_Consent_Template.docx
nih-grdr	NIH Global	Global Rare Disease Patient Registry and Data Repository (GRDR) consent is an agreement of a healthcare consumer to permit collection, access,

Access Control

- In der Regel basierend auf OAuth 2.0
  - Spezifikation lässt sehr viele Möglichkeiten offen
- Verschiedene Möglichkeiten der Implementierung
  - HL7 Implementation Guides
    - Smart on FHIR
      - Implementation Guide describes a set of foundational patterns based on OAuth 2.0 for client applications to authorize, authenticate, and integrate with FHIR-based data systems
      - http://www.hl7.org/fhir/smart-app-launch/index.html
    - UDAP - Security for Scalable Registration, Authentication, and Authorization (US-Realm)
      - implementation guide describes how to extend OAuth 2.0 and the HL7 SMART App Launch Framework using UDAP workflows
      - http://hl7.org/fhir/us/udap-security/2021Sep/
  - OpenID Heart
    - User Managed Access control using OAuth & FHIR
    - https://openid.net/wg/heart/
- See also: HL7 Version 3 Standard: Privacy and Security Architecture Framework - Trust Framework for Federated Authorization, Release 1 (four parts standard Includes provenance and audit)

Smart on FHIR Implementation Guide

- Definiert grundlegende Patterns für Authentifizierung, Autorisierung und Integration von Clients in FHIR basierte Systeme (z.B. EHR)
- Anbindung von Third Party Apps an EHR Systeme
- Berechtigungen über OAuth Scopes



Security Labels

- Konzept um Resourcen oder Bundles mit Security/Privacy relevanten Metadaten zu taggen
- Auswertung in der Regel von einer Access Control Engine
  - Empfängerseite
- Erfordert „Trust Framework“
- Kern Security Labels: Purpose of Use, Confidentiality, Sensitivity, Workflow (Delete After Use, No re-use ...)
- FHIR Data Segmentation for Privacy
  - https://build.fhir.org/ig/HL7/fhir-security-label-ds4p/

```
<Patient xmlns="http://hl7.org/fhir">
  <meta>
    <security>
      <system value="http://hl7.org/fhir/v3/Confidentiality"/>
      <code value="R"/>
      <display value="Restricted"/>
    </security>
  </meta>
...  [snip] ...
</Patient>
```

```
{
  "resourceType" : "Bundle",
  "type" : "searchset",
  ... other headers etc.....
  "entry" : [
     ... other entries ....
     {
       "resource": {
         "id" : "1",
         "meta" : {
           "security" : [{
             "system" : "http://terminology.hl7.org/CodeSystem/v3-ActCode",
             "code" : "DELAU",
             "display" : "delete after use"
           }]
         }
         ... other content etc.....
       }
     },
     ... other entries ....
  ]
}
```

Alissa Knight‘s report

“An effective kill chain in the targeting of the healthcare industry will not be of the EHR systems running in the providers, but in the third-party FHIR aggregators and third-party apps which access these EHR APIs as data moves from higher security levels to third-party aggregators where security has been found to be flagrantly lacking.”

“The findings in this report will show that of the three FHIR APIs I tested - which comprised an app ecosystem of 48 total FHIR apps and APIs and aggregated EHR data from over 25,000 healthcare providers and payers - contained pervasive authorization vulnerabilities that allowed me to access over 4 million patient and clinician records with my own patient login"

Playing With FHIR: Hacking and Securing FHIR APIs. https://approov.io/for/playing-with-fhir/

Alissa Knight‘s report

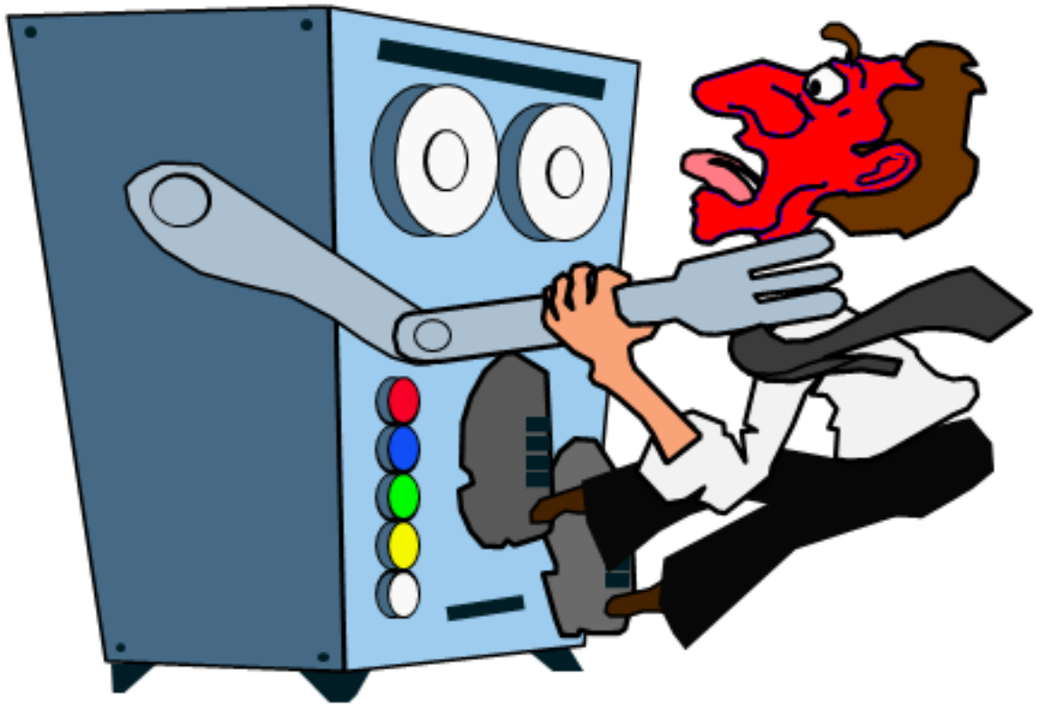
- Three production FHIR APIs serving an ecosystem of 48 apps and APIs were tested
- The ecosystem covered aggregated EHR data from 25,000 providers and payers
- 4m patient and clinician records could be accessed from 1 single patient login account
- 53% of mobile apps tested had hardcoded API keys and tokens which could be used to attack EHR APIs
- 100% of FHIR APIs tested allowed API access to other patient's health data using one patient's credentials.
- 50% of clinical data aggregators did not implement database segmentation allowing access to patient records belonging to other apps developed on their platform for other providers.
- 100 percent of the mobile apps tested did not prevent person-in-the-middle attacks, enabling hackers to harvest credentials and steal or manipulate confidential patient data.

Playing With FHIR: Hacking and Securing FHIR APIs. https://approov.io/for/playing-with-fhir/

Conclusion

- HL7 FHIR stellt Building Blocks und Guidances zur Unterstützung der Umsetzung von Security & Privacy zur Verfügung
- Die korrekte Umsetzung von Security auf allen ISO/OSI Layern obliegt dem Implementer
- Security Know How und Security(&Privacy) by Design helfen ungemein …

Danke für Ihre Aufmerksamkeit



References

- HL7 FHIR Security & Privacy guidance
  - https://hl7.org/fhir/security.html
  - https://hl7.org/fhir/secpriv-module.html
- HTTP Security
  - https://owasp.org/www-project-mobile-top-10/
- Application Security related
  - https://owasp.org/www-project-api-security/
  - https://owasp.org/www-project-top-ten/
  - https://owasp.org/www-project-mobile-top-10/