

FHIR Privacy and Security



FHIR Core

<http://bit.ly/FHIR-SecPriv>

John Moehrke (By Light)

<https://healthcaresecprivacy.blogspot.com/>

September 4, 2024



Agenda -- <http://bit.ly/FHIR-SecPriv>

Part 1 - Basics

- 🔗 Security Principles
- 🔗 Privacy Principles
- 🔗 Basic Security and Privacy Considerations
 - Anonymous Read
 - Business Sensitive
 - Individual Sensitive
 - Patient Sensitive
 - Not Classified
- 🔗 HTTP[S] - TLS
- 🔗 Authentication & Authorization
 - SMART on FHIR
 - IUA
 - Mutual-Authenticated TLS
 - UDAP
- 🔗 Access Denied Responses

Part 2 - FHIR capability

- 🔗 Provenance
 - Basic
 - Digital Signature
- 🔗 Audit Logging
 - Audit Reporting
 - Audit Purging
- 🔗 Consent - for Privacy
- 🔗 Permission (R6)
- 🔗 Signature
- 🔗 Attribute Based Access Control
 - Security Tags
 - Compartments / Clearance
 - Obligations
 - Break-Glass

Part 3 - Practical application

- 🔗 Provider Directory
- 🔗 Guide Management
- 🔗 Simple ABAC
- 🔗 Extra-Sensitive Treatment
 - Share with Protections
- 🔗 Proxy server to multiple
- 🔗 De-Identified Research
 - Re-Identification



John Moehrke

Architect: Healthcare Informatics Standards - Interoperability, Privacy, and Security

CyberPrivacy – Enabling authorized communications while respecting Privacy

IHE Co-Chair IT Infrastructure Planning & Technical Committee

HL7 Co-Chair Security WG, FHIR Management Group, FHIR facilitator, and FHIR Foundation founding member

Employee of ByLight Professional IT Services -- Contractor to VHA MyHealtheVet

JohnMoehrke@gmail.com | M +1 920-564-2067 | John.Moehrke@bylight.com

<https://www.linkedin.com/in/johnmoehrke> |

<https://healthcaresecprivacy.blogspot.com>

Twitter: [@JohnMoehrke](https://twitter.com/JohnMoehrke)

Courtney's third law: There are no technical solutions to management problems, but there are management solutions to technical problems.

Basics of Security and Privacy

HL7 CyberSecurity Event Recorder
<https://tinyurl.com/hl7sec>



Security

Management of Risks to:

- 🔗 Confidentiality
- 🔗 Integrity
- 🔗 Availability

Continuous Security

- 🔗 Patch Management
- 🔗 Revocation Checking
- 🔗 Active Backups
- 🔗 Database Integrity Checks
- 🔗 Audit Log analysis
- 🔗 Self-Testing - Postel's Law
- 🔗 Bug bounty programs

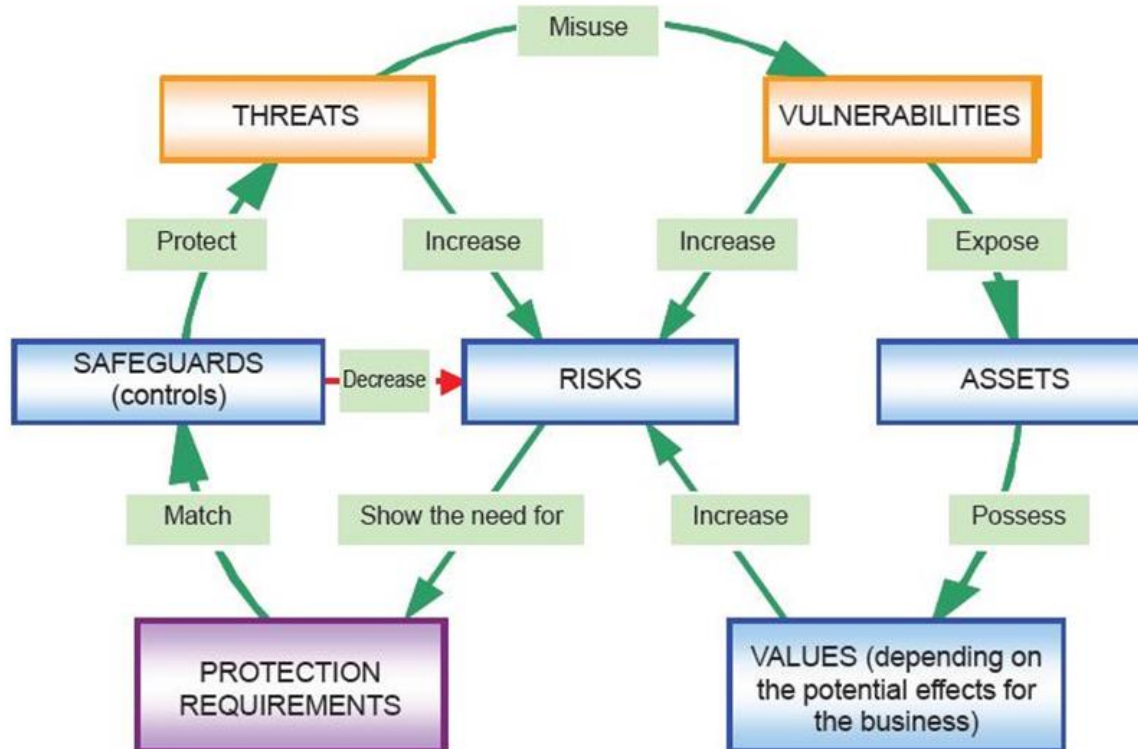
Security Capability Frameworks

- 🔗 NIST 800-53
 - NIST 800-171
- 🔗 HiTRUST
- 🔗 COBIT
- 🔗 OWASP
- 🔗 ISO 27001/27002
- 🔗 CIS Controls (formerly SANS Top 20)

Assessment Tools - e.g., Kali

- 🔗 API fuzzing
- 🔗 nmap - port scanner
- 🔗 Metasploit - exploitation framework
- 🔗 Uniscan - web app fingerprinting
- 🔗 Wireshark - packet sniffer
- 🔗 Burp Suite - web penetration testing
- 🔗 BeEF - browser exploit framework
- 🔗 Nessus - vulnerability scanner

Risk Management (ISO 13335)



Privacy Principles

The OECD Privacy Principles are as good as any to review

1. **Collection Limitation Principle**
2. **Data Quality Principle**
3. **Purpose Specification Principle**
4. **Use Limitation Principle**
5. **Security Safeguards Principle**
6. **Openness Principle**
7. **Individual Participation Principle**
8. **Accountability Principle**

Privacy by Design (PbD) - method to integrate Privacy Principles at design

Risks -- protecting resources

Wrong people get access

Right people get denied proper access

Right people see too much (consent)

Unauthorized Create/Update/Delete allowed

Right people get wrong data

Perception that wrong people got access

FHIR Security and Privacy Considerations

Grouping of similar risk tendency and use

1. Anonymous READ Access Resources
2. Business Sensitive Resources
3. Individual Sensitive Resources
4. Patient Sensitive Resources
5. Not classified - too many possibilities



Rubric not to be seen as mandatory

Healthcare is special

Most scale on Internet is one vendor at huge scale

→ Healthcare: Many organizations, divergent needs, ...

Most REST apps are User Managed, or Role Managed.

→ Healthcare: PurposeOfUse, Context, Safety, Sensitivity...

Most industries can remediate exposure: cancel credit card

→ Healthcare: once data are exposed it can't be revoked

Most industries can fix damages: insurance

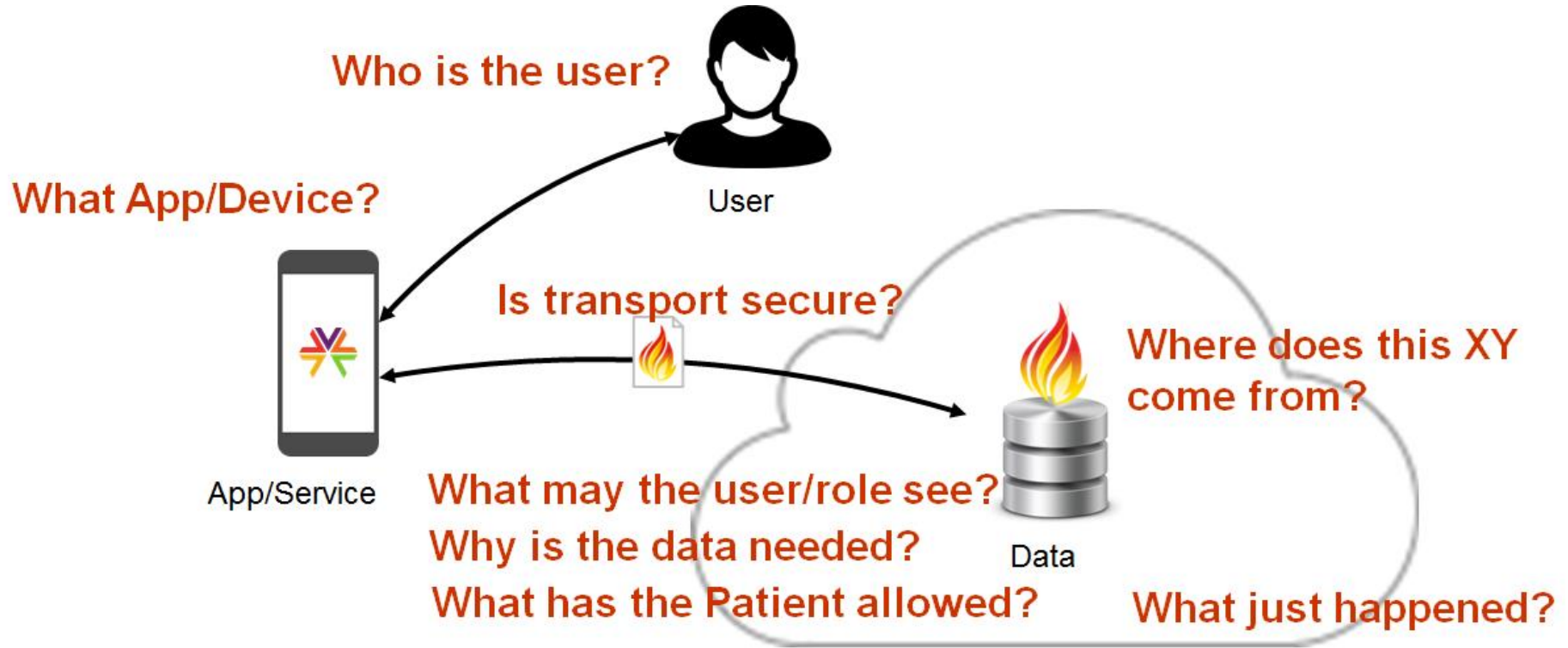
→ Healthcare: failure can cause death or long term pain

Healthcare should build on IT standards

- ⌘ Infrastructure - http, html, xml, json
- ⌘ Security - TLS, Certificates, OAuth, Signatures
- ⌘ Pluggable Authentication - OpenID Connect
- ⌘ Identity - leverage existing national ID
- ⌘ Coding - LOINC, SNOMED, RxNorm, etc
- ⌘ Models - REST, Document, Async, Streaming, Message
- ⌘ FHIR, CDA, XDS

Build on standards so you can focus on **adding value**

Security and Privacy needs



Basics of how? -- but not the only way...

Is transport secure?

https

Who is the user?

OpenID Connect

What App/Device?

OAuth client_id &

scopes

What may the user/role do?

Access Control rules

What the Patient authorized?

Consent Resource

Where does this data come?

Provenance Resource

What just happened?

AuditEvent

Secure Communications

TLS - 1.2 or higher -- See [IETF BCP 195](#)

- ⌘ Did you contact the intended server endpoint?
- ⌘ Was the communication authenticated?
- ⌘ Was the communication encrypted?
- ⌘ Was the integrity of the communication protected?

Best Current Practice for

- ⌘ HTTP -- [BCP 56](#)
- ⌘ OAuth -- not yet assigned a number, but [draft available](#) - draft-ietf-oauth-security-topics

Keith Boone - on TLS configuration

All found on <https://motorcycleguy.blogspot.com/>
June 2023 - August 2023

- ⑩ [TLS, FIPS and the Bouncy Castle Certified Encryption Module](#)
- ⑩ [Addressing technical challenges with BC-FIPS](#)
- ⑩ [Dynamically Reloading TLS Trust and Identity Material](#)
- ⑩ [Debugging TLS Protocol Failures in BC-FIPS and Spring Applications](#)
- ⑩ [TLS 1.2, Server Name Indication \(SNI\) and SOAP via CXF](#)

Access Control Considerations

- ⌘ App identity and authenticity
- ⌘ User Identity and authenticity
- ⌘ Context of request & Consent of subject
- ⌘ Basic CRUDE (Create, Read, Update, Delete, and Execute)

Poorly implemented Access Control can have negative impact on safety of patient and clinicians

Authentication and Authorization

Mutual-Authenticated-TLS

API Key

SAML SSO Profile

OAuth 2.0

Cascading OAuth

Open-ID Connect

User Managed Access (UMA)

SAML encapsulated

SMART-on-FHIR

SMART for Bulk Data Access

IHE Internet User Authorization (IUA)

HL7 - Scalable Reg, Authn, Authz
(UDAP)

HEART (a healthcare variant of UMA)

Access Control

Healthcare needs are complex

- ⌘ But leverage concepts: RBAC, ABAC, Policy, Context, Tags, Enforce Privacy Consents

- ⌘ special consent rules, episodic, expired, revoked

Data not simply classifiable into Role

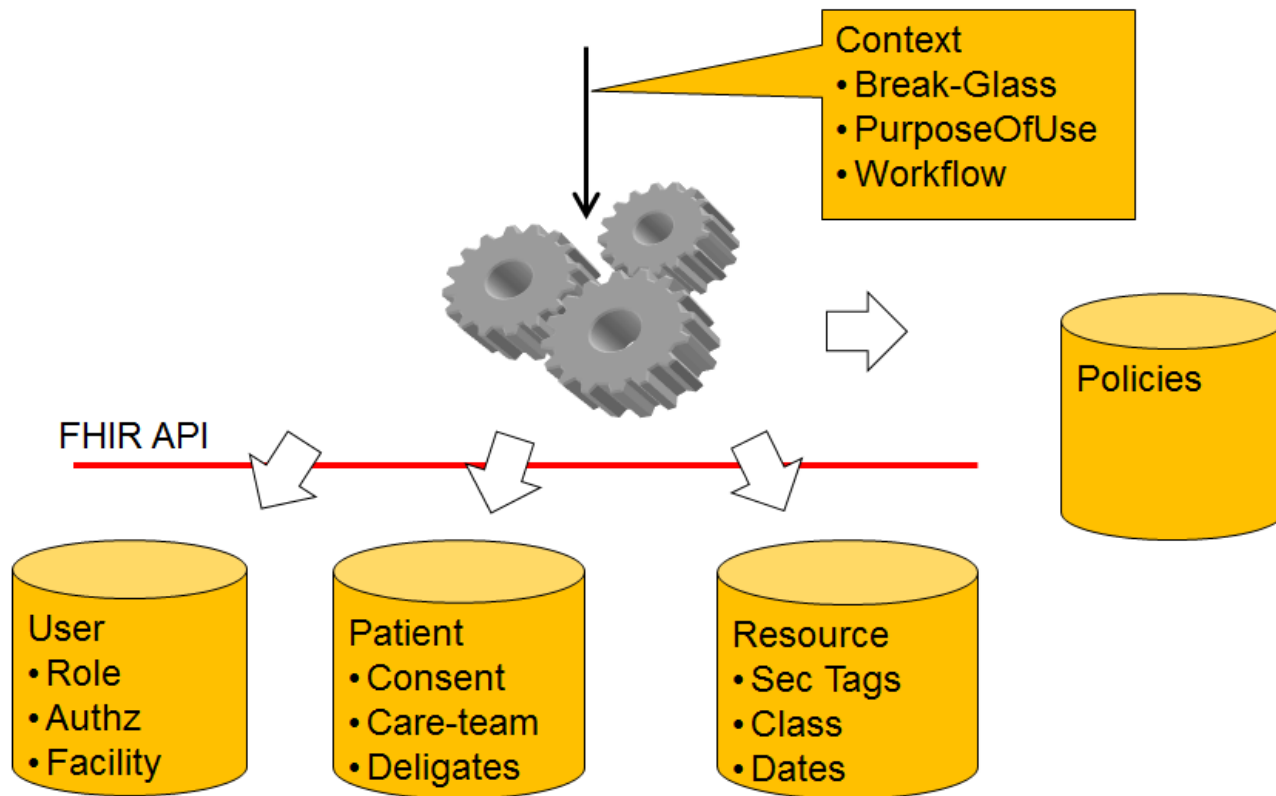
- ⌘ Leverage clinical types but need Security Tags

Policies point at data characteristics

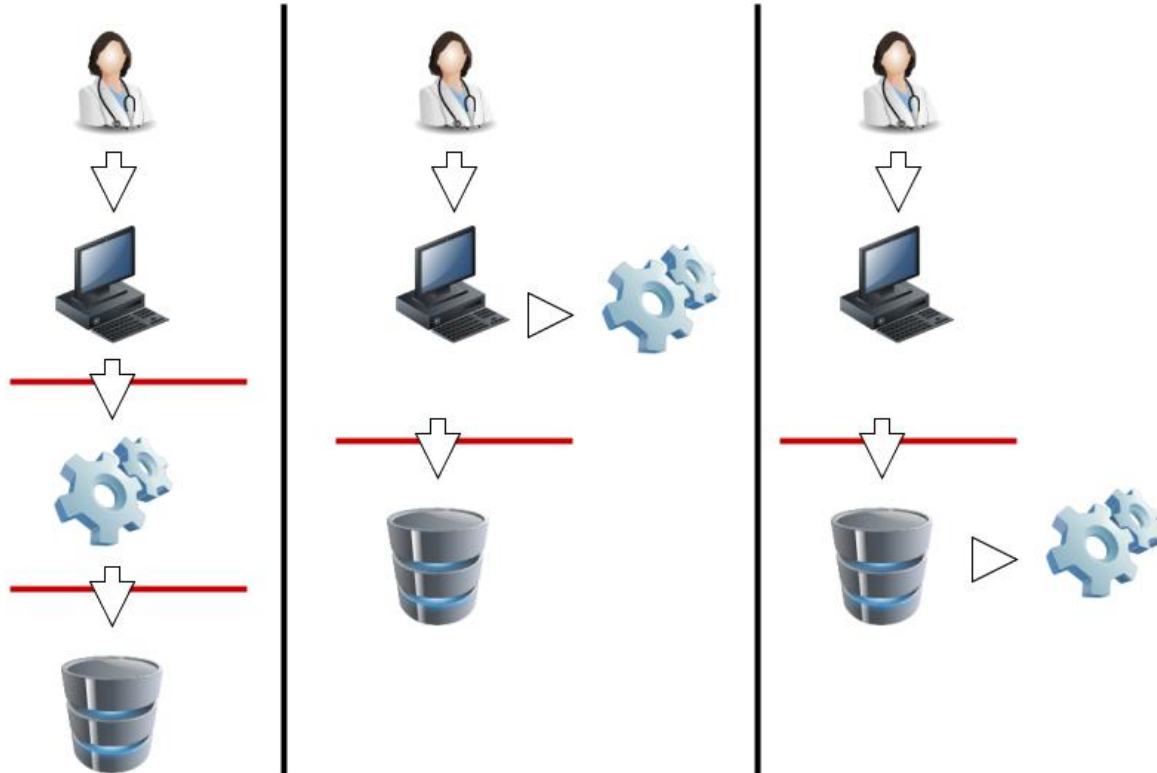
- ⌘ Sensitive Health Topics, Care-Team

Break-Glass – safety medical judgement

Access Control Engine



Deploying Access Control



OAuth - Permission - Scopes

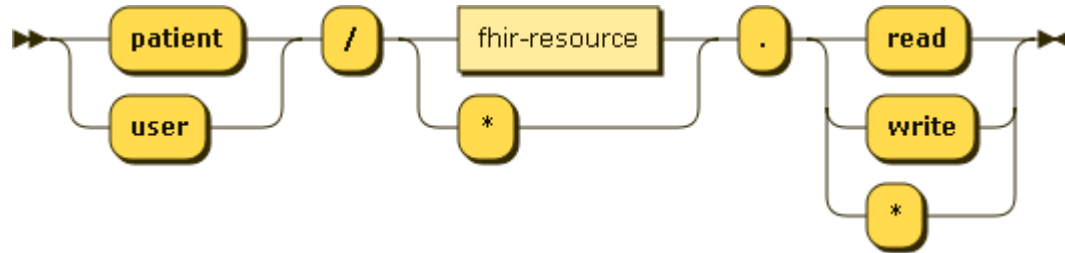
Scopes convey **what access** a service or app has authorized

- ⑩ “full access to your patient population”
- ⑩ “read-only access to one med list?”
- ⑩ “access to post new step counts?”

Allow that an app or service can ask for **less rights** than the user can be granted

Role-Based Access Control

🔗 Users → Roles → Permission (Resource+Action)



Example scope

for SMART on FHIR: Patient-level

Cardiac Risk app can ask for:

- ⑩ patient/**Patient.read**
- ⑩ patient/**Observation.read**

More complex Diabetes Monograph app:

- ⑩ patient/***.read**

An e-prescribing tool:

- ⑩ patient/**MedicationPrescription.write**

SMART - release 2

Enhancements and Clarifications to the SMART App Launch

🔗 Scope enhancements

- Full CRUDE support

- Finer-Grained resource constraints using search parameters
`patient/Observation.rs?category=laboratory`

🔗 Token Introspection

🔗 Server capabilities – .well-known/smart-configuration

🔗 etc...

<http://hl7.org/fhir/smart-app-launch/STU2/>

IHE-Internet User Authorization (IUA)

Focus is on Business-to-Business use-cases, less so end-user applications

- ✎ IUA promotes a loose coupling of Resource Server and Authorization Servers. This allows for deployments with multiple Resource Servers per Authorization Server as well as deployments with several or even no Authorization Servers.
- ✎ IUA supports a wide range of use-cases ranging from mobile application access to data, cross-enterprise data exchange to complex system integration scenarios.
- ✎ IUA is base-standard agnostic and can be combined with any HTTP RESTful transaction.
- ✎ IUA provides explicit means of obtaining access token claims from an access token by a resource server (with and without the involvement of an Authorization Server).
- ✎ IUA specifies additional authorization context claims such as BPPC consents and a user's organizational context.
- ✎ IUA provides explicit compatibility with IHE XUA.

<https://profiles.ihe.net/ITI/IUA>

Attribute-Based Access Control

Users-->Roles & Clearance & Context

Data selection rules selection rules on Attributes (elements)

⌘ Data selection rules may align with FHIRpath???

Rules specific to actions (CRUDE)

⌘ Search is a form of Execute

Policy orchestrates Users/Roles/Clearance with
Compartments/Resource/Attribute with Actions/Context

Resource.meta.security or any element

Access DENIED

Policy needs to weigh risks: -- Clients should expect all

Return a Success with Bundle containing zero results -

Return a 404 "Not Found" -

Return a 403 "Forbidden" -

Return a 401 "Unauthorized" -

Alissa Knight - White Hat Hacker

The New Healthcare Ecosystem will depend on FHIR APIs, but are They Secure?

My reaction

1. EHRs are doing a good job of securing their FHIR implementations
2. FHIR is good and worthy
3. There is room for improvement in some implementations
4. There are included recommended improvements.

Grahame's reaction

1. The report explicitly notes that no vulnerabilities were found or are documented in the EHR FHIR implementations themselves.
2. Nevertheless, lots of vulnerabilities were found. All of them are very basic house-keeping stuff well covered in the OWASP top ten risks.

Media Hype

1. Many media outlets did not get the facts right at all. Or even the impressions
2. Don't trust the media, read the report



Basic failure to secure

1. Resource-Server not enforcing scopes in the OAuth token

- Change the URL by the attacker (change the Patient id parameter)
- Given a read-only token, able to change data (change a medication of another patient)

2. Client/Server architecture where all data is sent to the Client

- A Patient Engagement App... the client was being used by a Patient on the Patients computer

3. Resource-Server not validating tokens

- Intercept a legitimate client app request, extract out the OAuth token, put that token into a request from your hacking client - so enforce timeouts and refresh cycles

4. Clients with hardcoded API keys in the app

Not hard for a hacker to decompile your app and find keys



Hack yourself before someone else does it for you

- 🔗 Your API or App will be attacked, better that you prepare
- 🔗 Look to cybersecurity experts - this is both a skill and an attitude
- 🔗 There are recommendations like from OWASP - <https://www.owasp.org/>
 - [OWASP top 10 API](#)
 - [OWASP mobile top 10](#)
- 🔗 Don't assume tokens are valid, don't assume token authorizes the request
- 🔗 Audit Logging of everything, and regularly inspect the logs for deviations
- 🔗 Provide a way for Vulnerabilities to be reported
 - Methods: <https://securitytxt.org/>, or <https://dnssecuritytxt.org/>, or <https://disclose.io/>
 - Expect issues to be reported, and be prepared (first response matters!)
- 🔗 OAuth and TLS have Best Current Practices written by experts

Security & Privacy Checklist

Fast Healthcare Interoperability Resources (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. This section gathers all information about security in one section. A summary:

1. **Time Keeping** - all clocks should be synchronized using NTP/SNTP, and the design of the system should be robust against a system clock with the wrong value
2. **Communications Security** - all exchange of production data should be secured using TLS (e.g., https).
3. **Authentication** - Users/Clients must be authenticated. For web-centric, OAuth is recommended. When using OAuth, a profile of OAuth will be needed. Consider use of **HL7 SMART-On-FHIR** where appropriate.
4. **Authorization/Access Control** - FHIR defines a Security Label infrastructure to support access control management. FHIR may also define a set of resources to administer access control management, but does not define any at present
5. **Audit** - FHIR defines **provenance** and **audit event** resources suitable for tracking the origins, authorship, history, status, and access of resources
6. **Digital Signatures** - FHIR includes several specifically reserved locations for digital signatures
7. **Attachments** - FHIR allows for binary resources and attachments. These have their own concerns
8. **Labels** - FHIR allows for set of security related tags that affect the way resources are handled
9. **Data Management Policies** - FHIR defines a set of capabilities to support data exchange. Not all the capabilities that FHIR enables may be appropriate or legal for use in some combinations of context and jurisdiction (e.g. HIPAA, GDPR). It is the responsibility of implementers to ensure that relevant regulations and other requirements are met.
10. **Narrative** - Care must be taken when displaying the narrative from FHIR resources
11. **Input Validation** - Validate all input received from other actors to assure the data is well formed and does not contain content that would cause unwanted system behaviour. Testing ensures that the input is not susceptible to data input validation errors by using techniques such as fuzzing, invalid input attacks, and injection attacks.
12. **When using OAuth** - Consider the draft **Best-Current-Practice for OAuth**
13. **Security / Privacy Event Reporting** - Consider legal obligations and ethical obligations to provide a means for Security and/or Privacy Event Reporting such as security vulnerability, or breach.

Part 2: FHIR core security and privacy

Provenance

- ⌘ Create / Update / Delete / Signed
- ⌘ Subject of Provenance is the data created/updated/deleted
 - .target
- ⌘ Audience is users of the data (not Privacy, Security, Ops)
- ⌘ Authenticity, Reliability, Trustworthiness, Integrity, Lifecycle
- ⌘ Not the only place where Provenance elements exist
 - FiveWs
- ⌘ May be overly exhaustively comprehensive
- ⌘ Basic Provenance -- Last-hop Custodian | Original Author

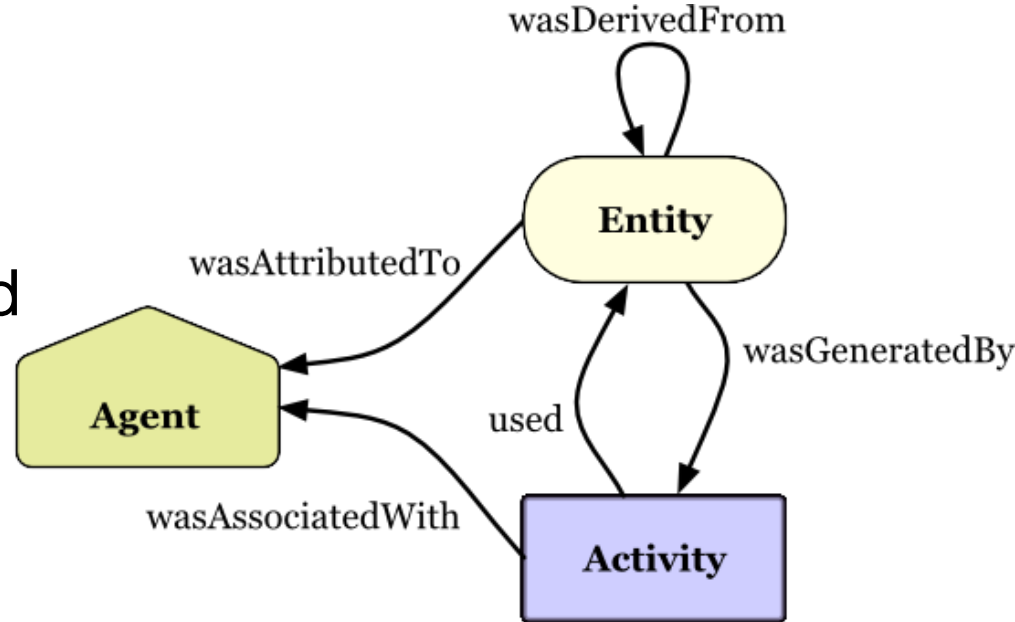
Provenance - model

Based on W3C Prov
(shown)

Except “Entity” is split

⌘ .target -- what was acted
upon / changed

⌘ .entity -- only what was
used



Provenance - tips

🔗 query/search on Provenance `target`

🔗 `_revinclude`







```
GET [base]/MedicationRequest?_revinclude=Provenance:target
```

🔗 X-Provenance

```
X-Provenance: { "resourceType": "Provenance", "location": {  
  "reference": "Location/1" }, "agent" ... }
```

🔗 Signatures - of the target

Profiles of Provenance

-  FHIR core - Relevant History
 - Minimal Provenance: when, why, and who made the change
-  EHR /PHR Record Lifecycle Events
 - minimal indicator of source Org
-  US-Core - Basic Provenance
 - Supporting provenance of
 -  Authorship - the author of the resource
 -  Transmitter - the last transmission (hop) from which received
-  IHE mXDE → link back to source Document
 - ... next page...

IHE mXDE use of Provenance

- ⑩ mXDE - Derive Resources from Documents (e.g. CDA or FHIR)
 - ⑩ Determine how often the FHIR resource data are referenced (1 vs many)
 - ⑩ Determine who has published the data
 - ⑩ Retrieve the Document to get full context
 - ⑩ Model for Provenance
 - One Provenance for each Document
 - Where a data Resource came from many documents, it will have many
- Provenance**
- **Provenance.recorded** when the decomposition happened
 - **Provenance.policy** = “[urn:ihe:iti:mxde:2023:document-provenance-policy](https://profiles.ihe.net/ITI/mXDE/index)”
 - **Provenance.agent** the software “assembler” that decomposed this document into these Resources
 - **Provenance.entity** the DocumentReference representing this document

AuditEvent

- ⌘ Security, Privacy, Workflow, and Operational events
 - Supports ANY event
- ⌘ Security Office investigations of security incident
- ⌘ Privacy Office investigations of privacy incident
- ⌘ Privacy Office support for Accounting of Disclosures...
- ⌘ Operations Office monitoring and efficiency
- ⌘ Not Provenance -- different audience and persistence
- ⌘ Not database journaling
- ⌘ Need to combine w/ proprietary logs (e.g. db, os, ...)

AuditEvent - based on many standards

The audit event is based on the IHE-ATNA Audit record definitions, originally from RFC 3881 , and now managed by DICOM (see DICOM Part 15 Annex A5).

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 – Defined the subset of audit events that an EHR would need

ISO/HL7 10781 EHR System Functional Model Release 2

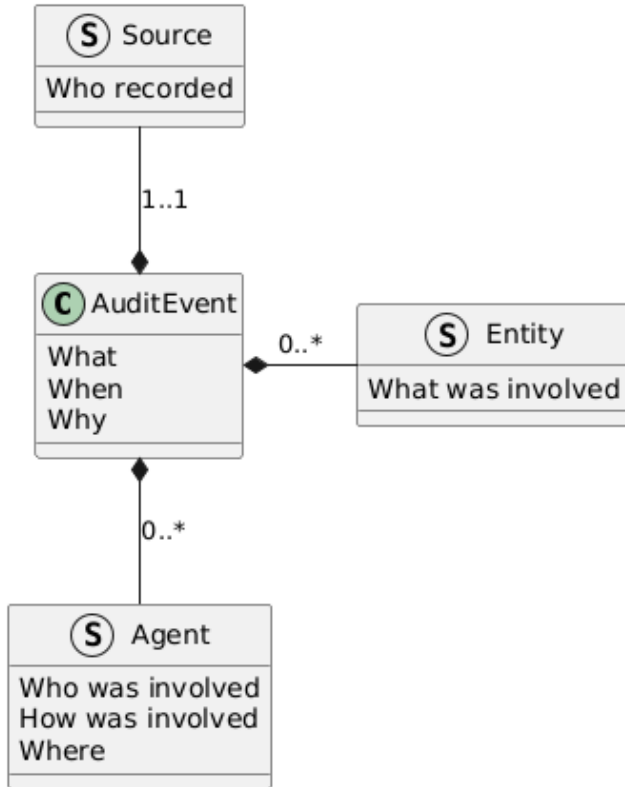
ISO 21089 Trusted End-to-End Information Flows

This resource is managed collaboratively between HL7, DICOM, and IHE.

AuditEvent - security & privacy events

- ⌘ System startup and shutdown
- ⌘ User login and logout
- ⌘ Application registration, authentication, authorization
- ⌘ Configuration Events
- ⌘ Installation of apps
- ⌘ Policy rules changes
- ⌘ Create/Read/Update/Delete of data (Resources)
- ⌘ Query/Search of data
- ⌘ Execute of Operations
- ⌘ etc.

AuditEvent - resource



Who - .agent(s)

What - .type, .subtype, .action

Where - .agent, .entity, .source

When - .period and .recorded

Why - .purposeOfEvent

Created - .entity(s)

Used - .entity(s)

AuditEvent - conformance

- ⌘ Most important to record that something happened
 - Failure to fill all the details should not stop recording
- ⌘ Fill as comprehensively as is reasonable
- ⌘ When you know the activity included a Patient (subject), record a .entity with that Patient id
- ⌘ Multiple recording sources
- ⌘ Logs may be purged on a regular basis after analysis
 - Logs analysis would look for unusual activity - alerts
 - Log reporting would result in permanent records
 - Offline archive

Basic Audit Log Patterns - Implementation Guide

<https://profiles.ihe.net/ITI/BALP>

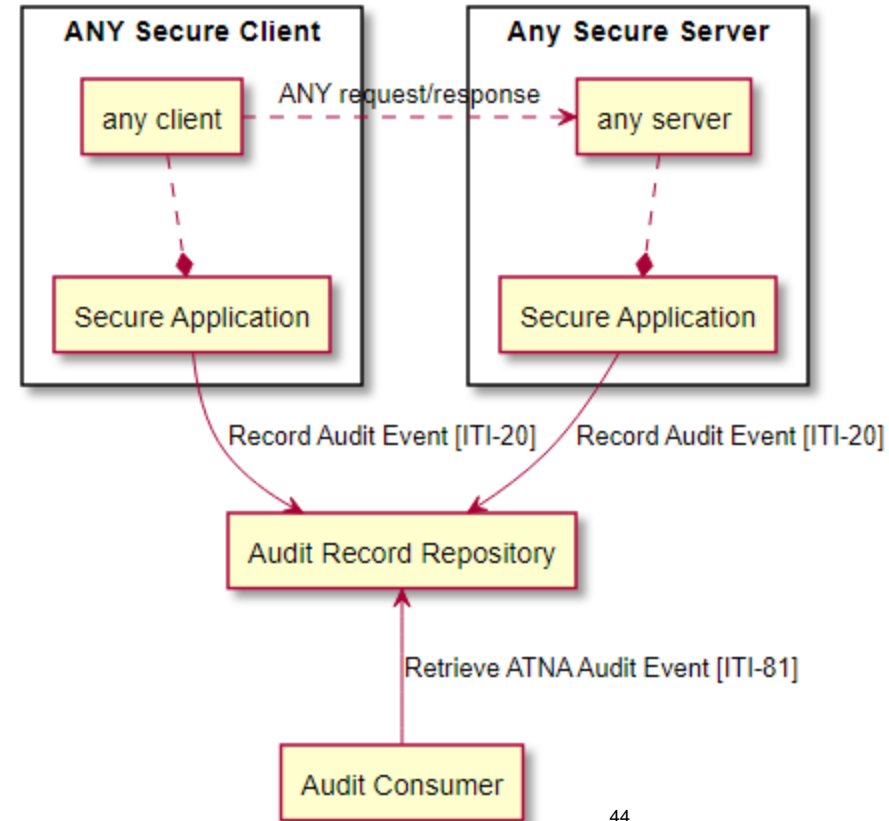
FHIR REST interactions

- 🔗 Create
- 🔗 Read
- 🔗 Update
- 🔗 Delete
- 🔗 Execute (search)

Linkage to Patient

OAuth & SAML decoration

Disclosure and Consent Decision



Platform Implementations of BALP

- 🔗 HAPI FHIR Server - https://hapifhir.io/hapi-fhir/docs/security/balp_interceptor.html
- 🔗 Firely FHIR Server - <https://docs.fire.ly/projects/Firely-Server/en/latest/security/auditing.html>

Consent - Privacy

Consent Resource - useful for many consent types

Positive and Negative - not just consent but dissent

Not just classic consent - also Authorizations

Depends on Local Policy meaning and enforcement

- ⌘ Just captures and records facts

- ⌘ Absence of a Consent means?

Questionnaire may be used in workflow to obtain Consent

Includes a RULE encoding customized to FHIR

Consent maturity

1. Consent resource just points at scanned paper
2. Consent resource just points at Questionnaire Response
3. Consent with encoded context
4. Consent with depth .provisions (PERMIT vs DENY)
5. Consent using external rules encoding (XACML)

Consent control vectors

- ⌘ Timeframe of validity of the consent - can expire
- ⌘ Organization consent applies to - data custodian
- ⌘ Who is being authorized (or denied)
- ⌘ Regulation consent applies to
- ⌘ Local Policy rules this consent build upon
- ⌘ PurposeOfUse - only this kind of use is allowed
- ⌘ Timeframe of data publication - only data in this period
- ⌘ Security Tags - sensitivity classification of the data
- ⌘ Type of clinical content - using clinical vocabulary use
- ⌘ Who authored the data - only data authored by

Basic Use-Cases

- ⌘ Consumer declaring their own desires (preferences)
 - Consent with empty .performer and .organization
- ⌘ Consent registry (file-cabinet with simply existence of paperwork). Supports knowing there is nothing vs something
 - Consent with .sourceReference, but no .provisions
- ⌘ Consent good for a period
 - Consent with .provision.period
- ⌘ Consent for specific purpose of use
 - Consent with .provision.purpose
- ⌘ Consent registry with Opt-In vs Opt-Out support only
 - Consent with .policy points at one or two policy
 - Consent with .provision.type and no other .provisions.

Consent

Type - permit/deny

Context affected

Actors affected

Data selection

Obligations

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 Group CareTeam Organization Patient Practitioner RelatedPerson PractitionerRole)	Resource for the actor (or group, by role)
action	Σ	0..*	CodeableConcept	Actions controlled by this rule Consent Action Codes (Example)
securityLabel	Σ	0..*	Coding	Security Labels that define affected resources SecurityLabels (Extensible)
purpose	Σ	0..*	Coding	Context of activities covered by this rule V3 Value SetPurposeOfUse (Extensible)
class	Σ	0..*	Coding	e.g. Resource Type, Profile, CDA, etc. Consent Content Class (Extensible)
code	Σ	0..*	CodeableConcept	e.g. LOINC or SNOMED CT code, etc. in the content Consent Content Codes (Example)
dataPeriod	Σ	0..1	Period	Timeframe for data controlled by this rule
data	Σ	0..*	BackboneElement	Data controlled by this rule
meaning	Σ	1..1	code	instance related dependents authoredby ConsentDataMeaning (Required)
reference	Σ	1..1	Reference(Any)	The actual data reference
provision		0..*	see provision	Nested Exception Rules

Consent profiling

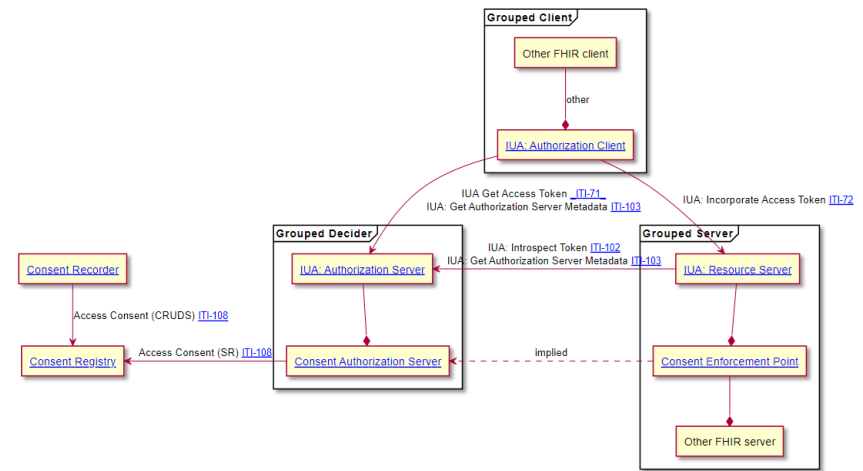


Figure 1:53.1-1: PCF Actor Diagram

IHE - Patient Consent on FHIR (PCF)

- <https://profiles.ihe.net/ITI/PCF>

Basic, Intermediate, Advanced

Hooks into OAuth flow

FAST Consent Management and SHIFT
are building upon PCF

Basic - Equivalent to IHE Basic Patient Privacy Consents

1. Identify who the Patient is
2. Identify what organization is being bound by this Consent
3. The Policy being acknowledged
4. Time period that the Consent is valid
5. When the Consent happened
6. What PurposeOfUse this applies to
7. Copy of the signed policy, which may be scanned ink-on-paper or other representation
8. Change of consent is done by Replacing previous

PCF: Privacy Consent complexity

- ⑩ Implied Consent
 - Basic-normal (TPO), all-normal, only-break-glass, deny-all
- ⑩ Explicit Basic Consent
 - Identified base policy, timeframe of the consent, who is authorized, who gave consent, what purposeOfUse
- ⑩ Explicit Intermediate
 - Data Timeframe, Data Id, Data Author, Data Relationship, and PurposeOfUse
- ⑩ Explicit Advanced
 - Reliant on a Security Labeling Service
- ⑩ And any combinations

Permission (Draft)

- ⌘ Define a permission (restriction) in a reusable form
- ⌘ May be used to indicate intent, or obligation
- ⌘ Leveraged by Consent
 - Useable beyond needs specifically recognized as “Consent”
- ⌘ Used for business-to-business communication of rules
 - Here is the data, you must not use it after 2 years.
- ⌘ Define access rules on data that is not patient specific
- ⌘ Define overriding base policy
- <http://build.fhir.org/permission>

Signature datatype

- ⌘ In Provenance, Contract, Bundle, VerificationResult
- ⌘ Rules for XML and JSON
- ⌘ Support for Electronic signature
- ⌘ Blockchain possibilities

```
{
  // from Element: extension
  "type" : [{ Coding }], // R! Indication of the reason the entity signed the object(s)
  "when" : "<instant>", // R! When the signature was created
  "who" : { Reference(Device|Organization|Patient|Practitioner|
    PractitionerRole|RelatedPerson) }, // R! Who signed
  "onBehalfOf" : { Reference(Device|Organization|Patient|Practitioner|
    PractitionerRole|RelatedPerson) }, // The party represented
  "targetFormat" : "<code>", // The technical format of the signed resources
  "sigFormat" : "<code>", // The technical format of the signature
  "data" : "<base64Binary>" // The actual signature content (XML DigSig. JWS, picture, etc.)
}
```

Security tags

🔗 Current use today limited to

- Treatment, Normal confidentiality

🔗 Used for:

- Resource header so consistently placed **.meta.security**
- Indicating sensitivity and confidentiality of **Resource**
- Indicating PurposeOfUse on **requests**
- Indicating Obligations/Constraints on **Content Bundles**

🔗 Data should not point at policy, policy should point at data

Security tags on data

Statement of “meta” about that data only.

- Security Labeling Service (SLS) may be used to inspect and tag

Not a **pointer** to policy, but rather a **classification** of the data

Data should not point at policy, policy should point at data

Vocabulary for use:

Healthcare Privacy / Security Classification System (HCS)

.meta.security

```
{  
  "resourceType" : "Bundle",  
  "meta" : {  
    "security" : [{  
      "system" : "http://terminology.hl7.org/CodeSystem/v3-  
ActCode",  
      "code" : "DELAU"  
    }],  
    {  
      "system" : "http://terminology.hl7.org/CodeSystem/v3-  
Confidentiality",  
      "code" : "R"  
    }  
  ],  
  "type" : "searchset",  
  ... other headers etc.....  
}
```

```
  "entry" : [  
    ... other entries ....  
    {  
      "resource": {  
        "resourceType" : "Observation",  
        "id" : "1",  
        "meta" : {  
          "security" : [{  
            "system" : "http://terminology.hl7.org/CodeSystem/v3-  
ActCode",  
            "code" : "ETHUD"  
          }],  
          {  
            "system" : "http://terminology.hl7.org/CodeSystem/v3-  
Confidentiality",  
            "code" : "R"  
          }  
        }  
      },  
      ... other content etc.....  
    }  
  ]  
}
```

Security tags- Implementation Consideration

Require policy domain rules to make the real

- ⌘ Which subset (ValueSet) vocabulary are to be used?
- ⌘ What do each code mean (behaviours)?
- ⌘ What is the absence of a value mean?
- ⌘ What does a code that is not understood mean?
- ⌘ Who authors (SLS?) Who can update?
- ⌘ Can subject specify some code values?
- ⌘ Maintaining codes received?
- ⌘ Operational implementations?

PurposeOfUse

In Requests → Intent to use results only for *this* purpose

In Response → Restriction to only use for *this* purpose

In Data → Data was captured only for *this* purpose

In Consent → Policy applying to *this* purpose

HL7 Defined Purposes are generally useful

 Structured in a hierarchy (ETREAT<TREAT)

Community may clarify standard codes or define own codes

Research is just a category, not a specific project

ConfidentialityCode

Privacy Risk classification on a non-overlapping scale

U -> L -> M -> **N** -> R -> V

In Treatment systems vast majority of data is “N” Normal

“R” - Mental Health, Sexual Disease, Drug/Alcohol Abuse

Once data has been de-identified it would be “U” or “L”

Emergency-Data-Set might be “M” or “L”

Bundle.meta.security confidentialityCode is always the
HIGHEST of the contents of the bundle (high-water mark)

Sensitivity Codes

Often only tagged data inside of an Organization

- ↳ Used for Access Control decisions
- ↳ Export strips these codes off as they expose sensitivity

Category of sensitivity -- so that Access Control rules could apply

- ↳ Segmentation by sensitivity category

Typical Codes:

- ↳ ETH, HIV, SCA, SDV, SEX/STD, PSY, SUD

VIP/CEL -- inappropriate use that still sometimes used

Obligations and Refrain

Not placed on data.

Found in Bundles -- as conditions of release

Found in Policies -- as conditions of Policy/Consent

Not typical - some useful:

- ⌘ DELAU - Delete After Use - can't persist the data
- ⌘ NORDSCLCD - No reDisclosure without patient consent
- ⌘ NOPAT - No Disclosure to Patient without provider auth
- ⌘ NOREUSE - Do Not Re-Use - can't redistribute the data
- ⌘ HTEST - Test Data - marks data that is not real but test

Clearance and Compartment

Data are grouped into one or more compartment(s)

Users are permissioned with one or more clearance(s)

Compartment -- Similar but not the same as REST

- ↳ Tend to be Project names

- ↳ Not common in Treatment

- ↳ Most used in Research 'projects'

No pre-defined vocabulary

Authorization is when Compartment is within Clearance(s)

Integrity Category

Not in common use

completeness, veracity, reliability, trustworthiness

Useful Terms

⌘ Patient Reported

⌘ Payer Reported

⌘ Professional Reported

⌘ Subsetted -- used in FHIR when summary requested

⌘ Abstracted / Aggregated

⌘ De-Identified or Pseudonomized

FHIR Data Segmentation for Privacy

Implementation Guide released Standard for Trial Use

<https://hl7.org/fhir/uv/security-label-ds4p/>

- ⑩ Background
- ⑩ Security Labeling Conceptual Structure
- ⑩ Detailed Specification
- ⑩ Inline Security Labels
- ⑩ Artifacts Index
- ⑩ Security and Privacy Considerations
- ⑩ Glossary

Break Glass - one possibility

In **Treatment** use-cases there are times when an **Authorized Clinician** can declare a **Safety override** of **Privacy** restrictions

- ⌘ Break-Glass declaration should trigger Privacy Office
- ⌘ NOT Emergency Department use normal use

```
HTTP/1.1 GET fhir/Patient/482735/condition
Content-Type: text/xml
Access-Control-Allow-Origin: *
Last-Modified: Thu, 19 Nov 2013 07:07:32 +1100
ETag: 24
```

```
Category: http://terminology.hl7.org/CodeSystem/v3-ActReason#BTG; scheme="http://hl7.org/fhir/tag/security"; label="break the glass"
```

Part 3: Use-Case Practical Application

Multiple Organization - Provider Directory

- Endpoint
- Location
- Organization
- Practitioner
- PractitionerRole



Permission to Create & Update

Central authority must create Organization

- Organization

Create must come from a trusted organization

- Location, Endpoint, PractitionerRole, Practitioner*

- Practitioner should not be duplicated, so use if present

Update must come from THE organization related

- Points at Organization

Practitioner may be pointed to by many PractitionerRole

Attribute Based Access Control

Attribute in this case is the relationship to Organization

Direct Link:

- 🔗 Location.managingOrganization
- 🔗 Endpoint.managingOrganization
- 🔗 PractitionerRole.organization

Indirection

- 🔗 PractitionerRole.practitioner

Multiple Organization - Profile Directory

Use-Case: Collaboration on Guides

Users manage Teams of Users that have authorization to Projects

- ↳ Projects --> Compartment
- ↳ Team Membership --> Clearance
- ↳ All data meta.security tagged (1..*) Compartment
- ↳ Permit user with team membership (clearance) to one of the projects (compartment) that the resource is tagged
- ↳ Otherwise deny a Create/Update/Delete request

Implementation

Create requests -- data is tagged with project compartment

- ⌘ Client specifies compartment or,
- ⌘ Server uses compartment from user clearance
- ⌘ Thus Resource.meta.security to compartment

Update to add other projects

- ⌘ User from current project can update to add other project

Delete ???

Attribute Based Access Control

Attribute in this case is *.meta.security

Thus Access Control enforcement does not need to deeply inspect the data, or know what kind of resource it is

Team membership could be managed as classic “Role”

⌘ But is formally in ABAC is called a “Clearance”

Could be implemented with FHIR Group resource

Simple use of .meta.security

Using .meta.security for license

Some codeSystems have licensing requirements, some are fully open. [zulip chat](#)

Ontoserver supports per-CodeSystem security labels. So you could flag a bunch of things as requiring a UMLS licence and then other things with a separate licence.

Simple use of ABAC in Clinical Use

VIP Patient

Given that not all Clinician users would be granted access to VIP patients:

- a. Each User granted authorization would be granted access to VIP Clearance
- b. Each Patient that is additionally protected as a VIP would be tagged with VIP Compartment

Thus any access by a User to any data associated with a Patient must have $\text{Clearance(VIP)} == \text{Compartment (VIP)}$

⌘ Search on Patient would have VIP patients removed from the result when the user does not have VIP clearance.

⌘ Good start, but not sufficient

Extra-Sensitive Data sharing with Protection

Today Health Information Exchanges

Exchange network is Restricted by definition to Treatment
Expect Custodian to not release unless authorized to release
All data is considered Normal Healthcare Sensitive
No differentiation of Extra-Sensitive information

Thus: many will not release Extra-Sensitive information as
there is no expectation it will be treated as Extra-Sensitive.

Extra-Sensitive - Trust Domain

Agreement to abide by defined rules (Contract) within a trust domain, with defined breach ramifications

- ⌘ Meaning of PurposeOfUse codes
- ⌘ Meaning of ConfidentialityCode codes
- ⌘ Meaning of Sensitivity codes
- ⌘ Definition of Responsibilities
- ⌘ Definition of Trust Identities
- ⌘ Definition of Communications
- ⌘ Definition of Consent handling

PurposeOfUse - Context of a request/response

Treatment - Medical treatment of subject with legitimate relation by those holding clinical credentials at trusted treatment organization

Emergency Treatment - Authorized Clinical agent has declared a potential patient safety situation (Break Glass)

Payment - Payment and Coverage with legitimate payers holding a relationship with the subject and with subject's authorization (non denial of access)

Operations - Maintenance and Legal/Regulated actions

Public-Health - Legal/Regulated actions to protect public health (e.g. Immunization Registry, Prescription Drug Monitoring Program)

Research - Clinical Research under a defined trusted project. Must be accompanied with trusted project clearance identification

Extra-Sensitive

Defined meaning to subset of confidentiality and sensitive codes

- ⌘ Normal - Normal healthcare sensitive information requiring clinical need and to be shared only for Treatment
- ⌘ Restricted - Extra-Sensitive healthcare information requiring clinical need-to-know subject to break-glass and not to be shared externally without Explicit-Consent
- ⌘ Subset of Extra-Sensitive sub-class: ETH, STD, MH, ...

Security Labeling Service

Service that could be used to tag data

🔗 Batch, create/update, or export/use

Inspects the data, possibly deep inspection

Charged with medical rules (likely Clinical Decision Support)

Tags data using “Sensitivity” codes

🔗 As representative grouping (classifications) of sensitivity

May tag elements, or whole Resources

Rules may change over time (batch)

Least Privilege and Segmentation of Duties

Everyone must persist tags (especially those on imported)

Everyone must segment their Users to enable this

Defined Training and Responsibilities -- authorizations

- Classed by Treatment vs Payment vs Operations

- Class of users enabled for Extra-Sensitive

- Defined mechanism for Break-Glass

Follow up investigation of all Break-Glass

Patient is authorized to Access Log Accounting

Shared with Permissions

Request -

Assertion

User Identity

OnBehalf of Organizational

PurposeOfUse

Clearance | Roles

Promise

Request Parameters

Response-

Bundle.meta.security -

High-Water mark - (confidentialityCode +
sensitivity)

Obligations - do not reDisclose

May have regulation identification (42 CFR Part
2)

Authorized PurposeOfUse

Resources.meta.security -

Specific confidentialityCode

May have sensitivity classification

Trust but Verify

Right of inspection

Random inspections

Audit Log -- AuditEvent will be recording all uses of data

Performance and Service Level

Failures must have consequences

Multiple-Servers with one proxy

Complexity

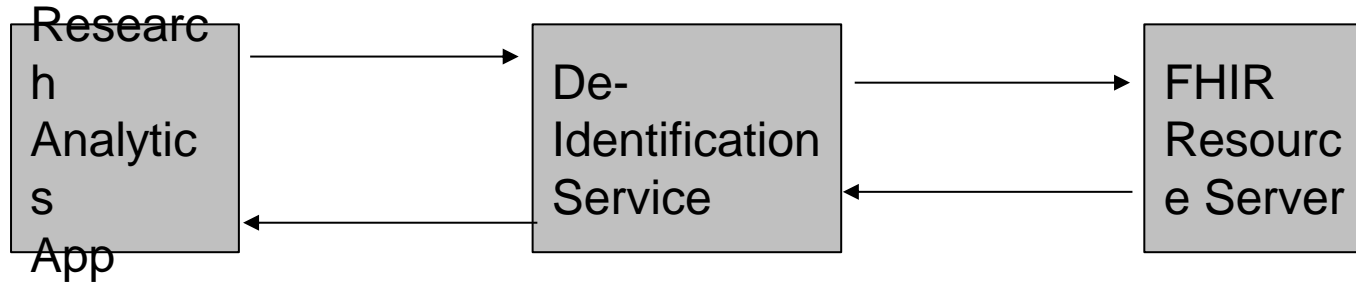
WhitePaper draft -

<https://confluence.hl7.org/display/FHIR/Intermediaries+White+Paper>

- ⌘ Managing Access Rights & Security
- ⌘ Identification / references
- ⌘ Combining Search results
- ⌘ Inconsistent record keeping
- ⌘ Distributed business logic

Research

Orchestration of Services



Cascade of OAuth tokens so that the Resource Server has assurance data will be De-Identified

Data Tags indicate De-Identification is a requirement

Data Tags indicate Data has been De-Identified

De-Identification

De-Identification = Anonymization | Pseudonymization

Lowers Risk of Identification or Re-Identification

Algorithm customized to **risk** & ultimate data use-case **need**

⑩ null, static, fuzzing, masking, pseudonym, generalize, etc

Some identifiers in Observation Resource:

⌘ Direct Identifiers: .identifier, .subject, .performer, .encounter, .focus, .note, .specimen, .basedOn

⌘ Indirect Identifiers: .category, .code, .issued, .effective[x], .method, .bodySite, .interpretation, .value[x], .component

Patient Data Embargo Management

[blog](#)

Provenance vs AuditEvent

Provenance as linkage to source

Mostly Medical Records use-cases

- 🔗 Use in Reconciliation process
- 🔗 Use in Data Element extraction from Documents
- 🔗 Use in Export of data to another organization

Security use-case tends to rely on AuditEvent

Privacy reporting tends to rely on AuditEvent

Conclusion

Questions?

Ongoing Discussion:

- <https://chat.fhir.org> Security & Privacy Stream
- [HL7 Security Workgroup](#)
 - FHIR Security call on Mondays 12 noon eastern

John Moehrke

JohnMoehrke@gmail.com

<http://healthcaresecprivacy.blogspot.com>