HL7 GDPR on FHIR

FH-Prof. DI Alexander Mense, CISSP, CISA
Co-chair HL7 International Security WG

FH University of Applied Sciences TECHNIKUM WIEN

HL7 AUSTRIA

Agenda

- HL7 FHIR Security & Privacy artefacts
- Example
- HL7 GDPR Whitepaper

HL7 - Security & Privacy

- HL7 defined several components to support implementation of security & privacy
  - CDA elements
  - FHIR components
    - Resources, Guidance, Vocabulary
  - General security guidance

HL7 FHIR Security & Privacy

Structure | UML | XML | JSON | Turtle | R2 Diff | All

Structure

Name	Flags	Card.	Type	Description & Constraints
Consent	I		DomainResource	A healthcare consumer's policy choices to permits or denies reci purposes and periods of time *+ Either a Policy or PolicyRule* Elements defined in Ancestors: id, meta, implicitRules, language
identifier	Σ	0..1	Identifier	Identifier for this record (external references)
status	?! Σ	1..1	code	draft | proposed | active | rejected | inactive | entered-in-error ConsentState (Required)
category	Σ	0..*	CodeableConcept	Classification of the consent statement - for indexing/retrieval Consent Category Codes (Example)
patient	Σ	1..1	Reference(Patient)	Who the consent applies to
period	Σ	0..1	Period	Period that this consent applies
dateTime	Σ	0..1	dateTime	When this Consent was created or indexed
consentingParty	Σ	0..*	Reference(Organization | Patient | Practitioner | RelatedPerson)	Who is agreeing to the policy and exceptions
actor	Σ	0..*	BackboneElement	Who|what controlled by this consent (or group, by role)
role		1..1	CodeableConcept	How the actor is involved SecurityRoleType (Extensible)

HL7 FHIR Security & Privacy

- Resources
  - Consent
    - Express consent regarding healthcare
    - Currently Privacy consent directive is well defined: agreement to collect, access, use or disclose (share) information
    - Enables capturing, storing, transmitting simply to complex privacy policies
    - http://hl7.org/implement/standards/fhir/consent.html
  - Provenance
    - describes entities and processes involved in producing and delivering or otherwise influencing a resource.
    - Provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility
    - based on the W3C Provenance specification
    - http://hl7.org/implement/standards/fhir/provenance.html

HL7 FHIR Security & Privacy

- Resources
  - Audit Event
    - record of an event made for purposes of maintaining a security log
    - based on the IHE-ATNA Audit record definitions, originally from RFC 3881 , and now managed by DICOM
    - actors - such as applications, processes, and services - involved in an auditable event should record an AuditEvent
    - http://hl7.org/implement/standards/fhir/auditevent.html

HL7 FHIR Security & Privacy

- Implementation Guidance & Principles
  - Security Labels
    - concept attached to a resource or bundle that provides specific security metadata about the information
    - Context of Use
      - Purpose Of Use
    - Data Sensitivity
      - Confidentiality codes
    - Control Flow
    - http://hl7.org/implement/standards/fhir/security-labels.html

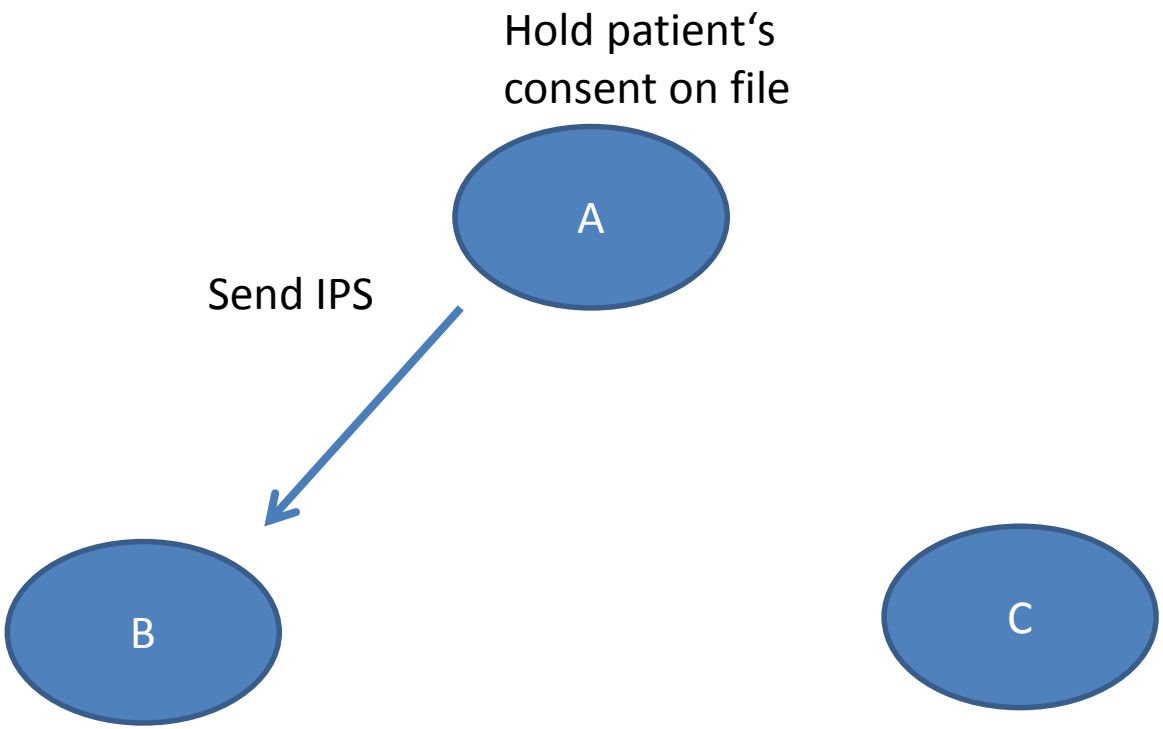
HL7 FHIR Security & Privacy

- Implementation Guidance & Principles
  - Security Principles
    - Secure Communication
    - Authentication
    - Authorization / Access control
    - …
    - http://hl7.org/implement/standards/fhir/security.html

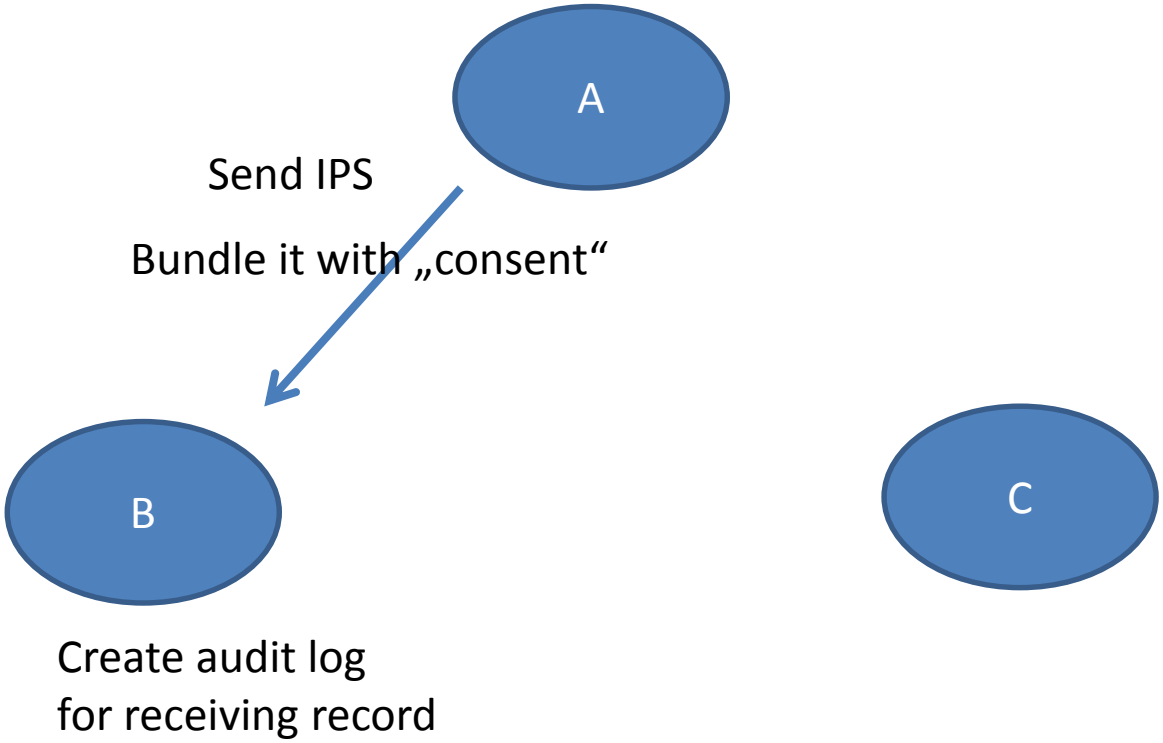
HL7 FHIR Security& Privacy

- Vocabulary
  - Purpose Of Use
    - Currently adopted according to GDPR art. 6 & 9
  - confidentiality classesification
  - InformationSensitivityPolicy
  - …

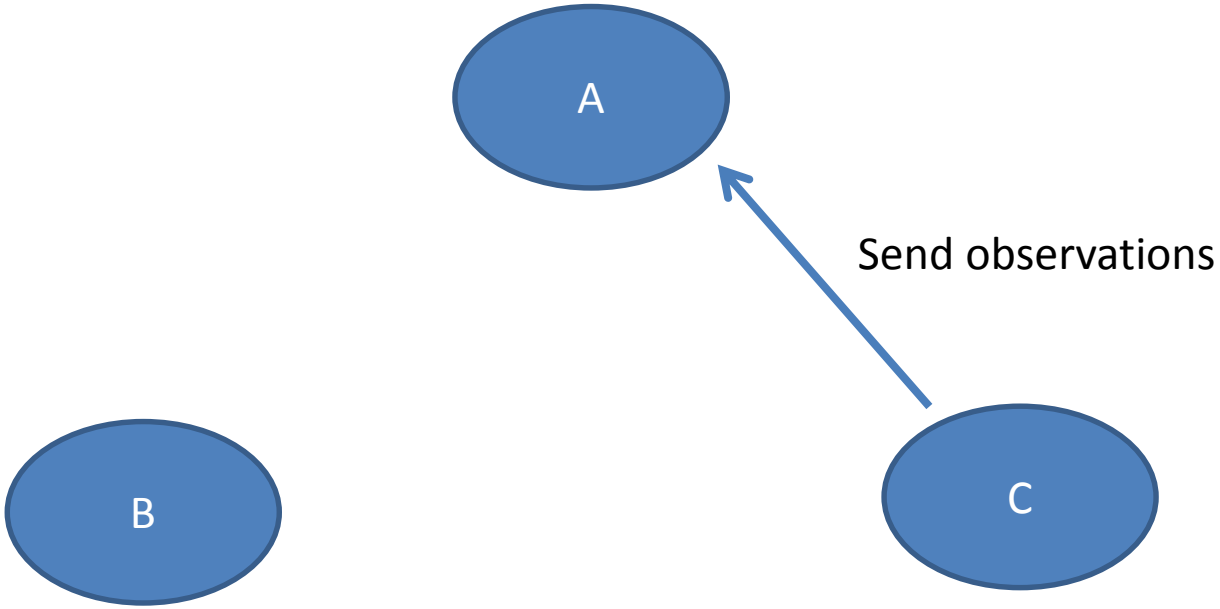
Example



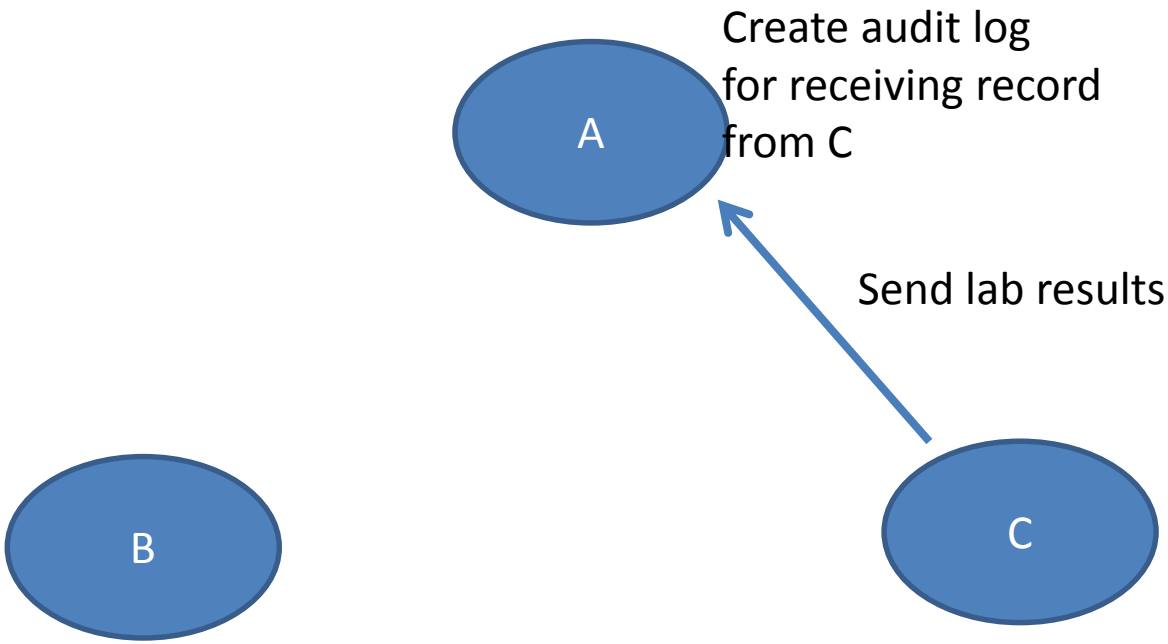
Example



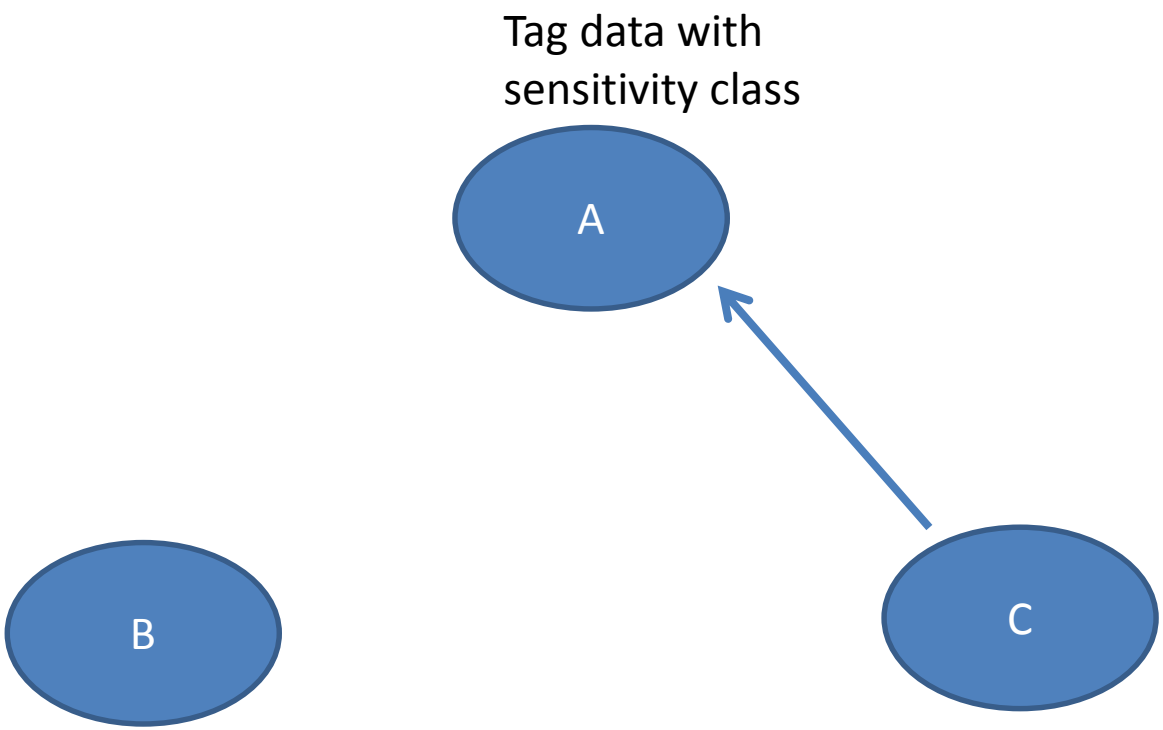
Example



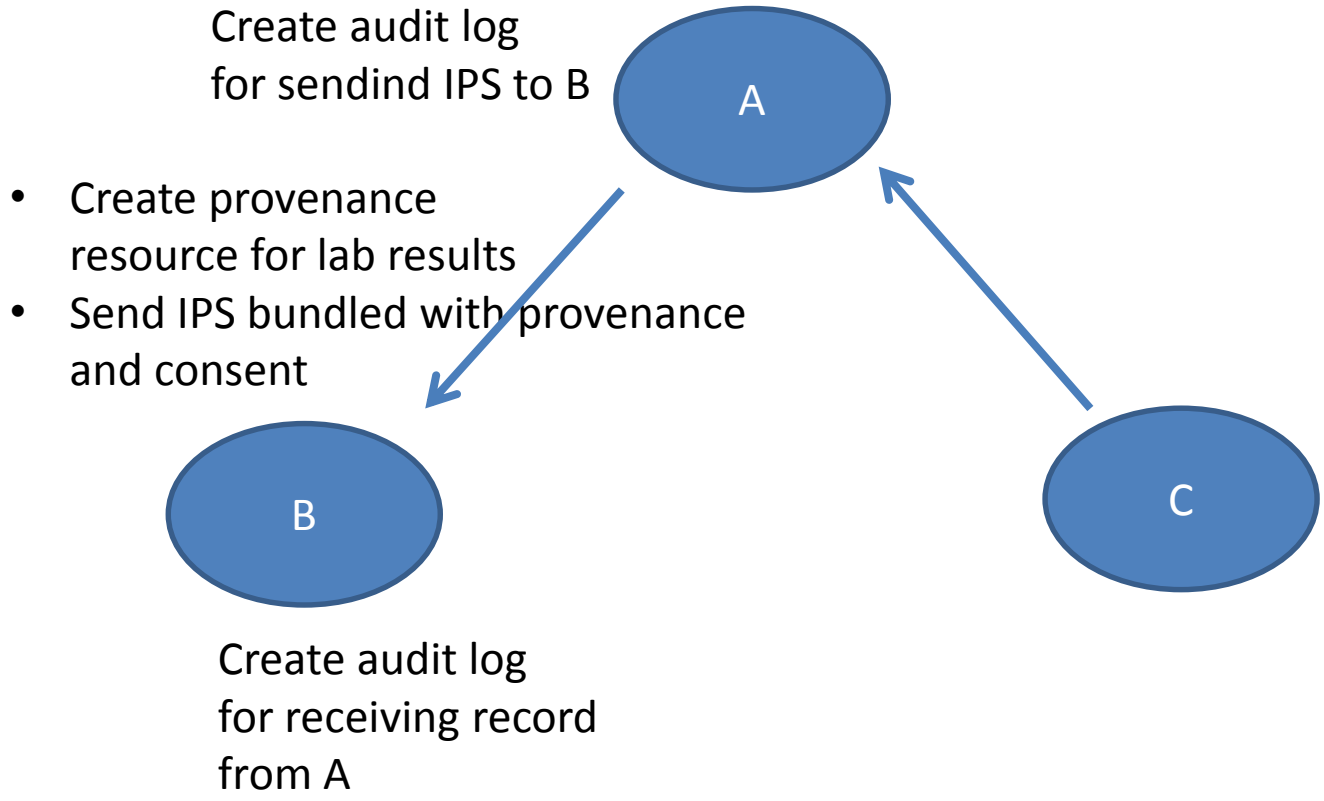
Example



Example



Example



HL7 GDPR Whitepaper

- Goal: Provide guidance how HL7 FHIR components support implementation of GDPR requirements
- General principles
  - Focussed on FHIR / technical level
  - No specific policies
  - No legal assumptions
- Work in progress
  - https://confluence.hl7.org/display/SEC/FHIR+-+GDPR
  - Weekly ConfCall

HL7 GDPR Whitepaper

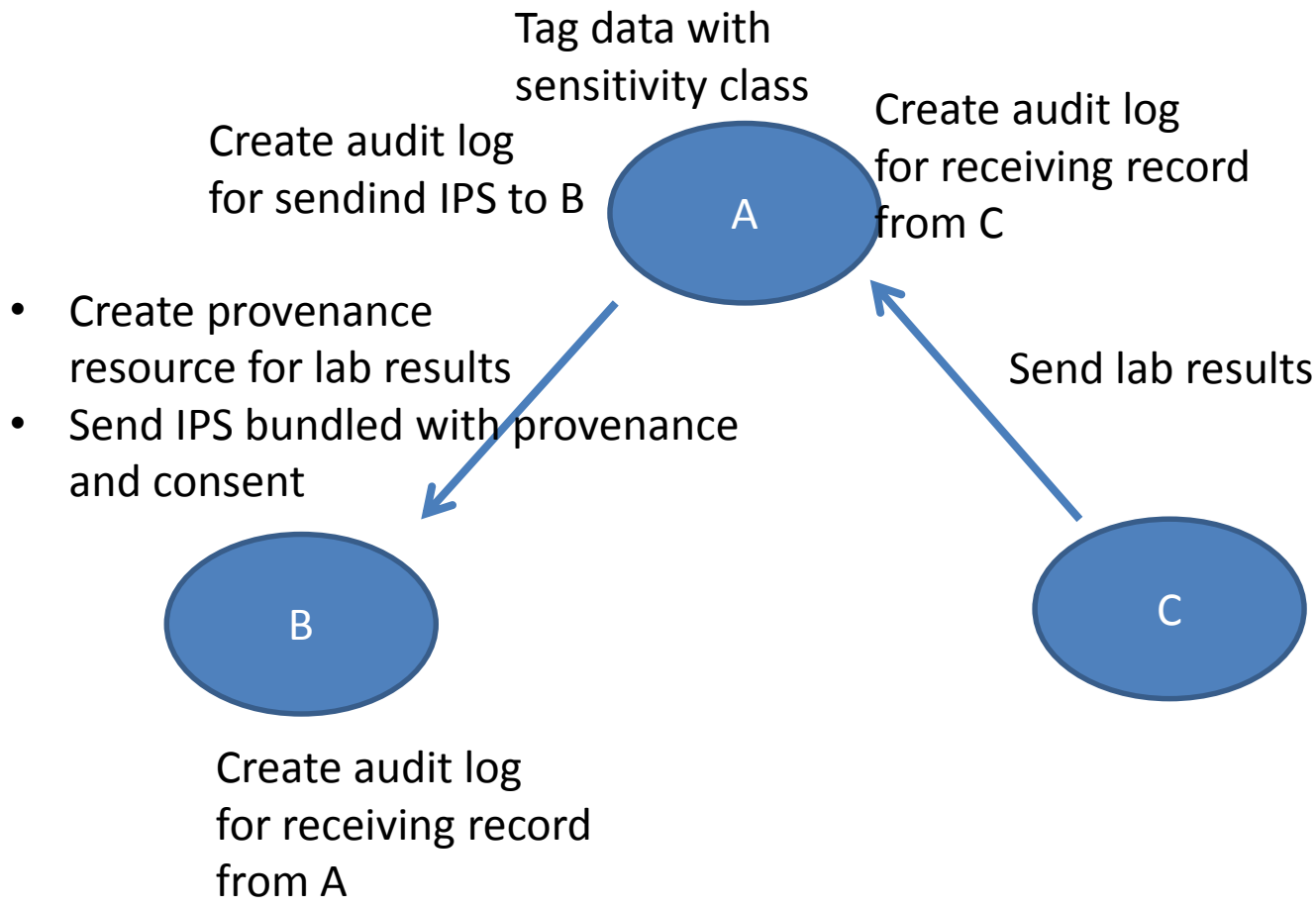
- Requirement for explicit consent …
  → The consent resource might be used to hold specific consent on file or to send information about given consent along with healthcare information.
- Requirement for transparency …
  → means a controller needs to keep track of the processing of personal data and provide information. To store information about data sources either AuditEvent or Provenance can be used …

HL7 GDPR Whitepaper

- Work progress
  - Mapping Requirents of GDPR to existing components (e.g. resources, security labels, vocab, …)
  - Identify gaps
  - Provide „whitepaper“
  - Provide simple examples
  - Propose future work items to be done by HL7

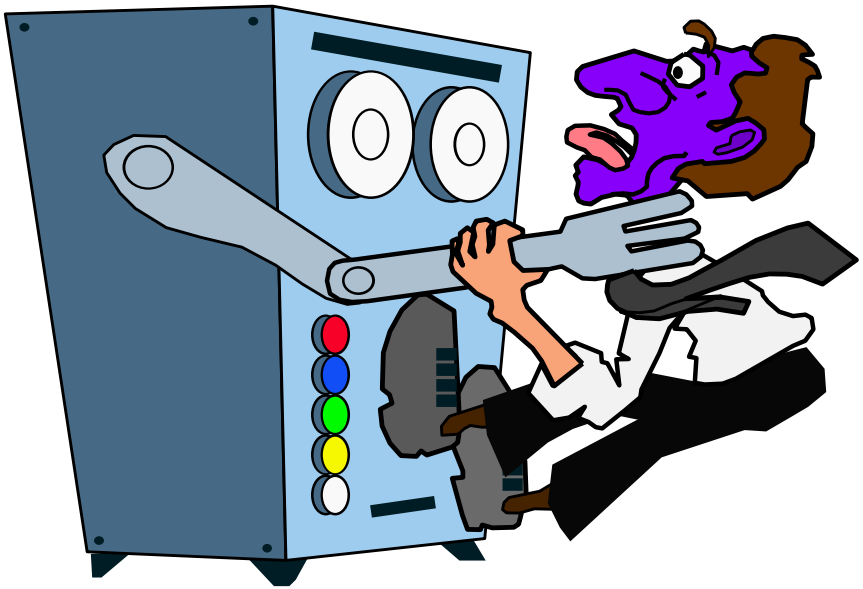
- Examples
  - It‘s planned to include examples – handling IPS might be a complex one
  - but probably already bound to specific policies?

Example



- Create provenance resource for lab results
- Send IPS bundled with provenance and consent

Thanks for your attention



alexander.mense@hl7.at