# GDPR Impact on Cross-Border Sharing of CDA Documents

**Stéphane Spahni**

**Presented by Karima Bourquard**

**GDPR and IPS Workshop**

**Brussels, September 13, 2018**

# National Contact Point for Cross-Border Exchange

@ Speaker twitter handle

- Project started in 2008 under the name “epSOS”
- Service provision being established under CEF CBeHIS
  - Go-live waves in 2018, 2019, 2020
- Integration with other CEF building blocks: CEF PKI, CEF eDelivery, CEF eID
- Objective: reliable exchange of information between countries
  - Including transcoding and translation of documents
  - Without intervening into national infrastructure
  - Through the establishment of a circle of trust between the countries
- Use cases (based on epSOS specifications)
  - Patient Summary
  - ePrescription / eDispense

# The National Contact Point for eHealth (NCPeH)

- Bi-directional Gateway in each country
- Umbrella for
  - Legal aspects → NCPeH organization is the legal umbrella for the country
  - Semantic aspects → NCPeH is in charge of semantic interoperability
  - Organizational aspects → NCPeH is the single point of contact for the whole country
  - Technical aspects → NCPeH "speaks" CEF on one side and "national" on the other side
- Possibly two-ways
  - Acts as "Country A" → connected to the national Electronic Patient Record (EPR) infrastructure
  - Acts as "Country B" → connected to healthcare providers portals

# Legal aspects

- Circle of trust
  - Legal agreement between countries (National Authorities)
  - Addresses operational aspects

- Patient Information Notice (detailed privacy information for the patient)
  - At country A level (country of origin)
  - At country B level (country of care / of healthcare professional)
  - Informed Consent for Patients
  - Addresses personal data protection aspects

- Traceability
  - ATNA Logs at Country A and Country B
  - Non-repudiation assertions

# Legal Agreement

- Establishes the necessary legal framework between National Authorities
- Establishes the basic rules for operating a National Contact Points
- Establishes the basic rules for the identification and authentication of patients and healthcare providers
- Establishes the basic rules related to the processing of personal data
- Establishes the basic technical rules related to security, traceability, audit and non-repudiation

# The *Model* Patient Information Notice (Model PIN)

- Template for informing citizens / patients about their data protection rights
  - National customization required
- Use recommended by Article 29 Working Party on Data Protection
- Addresses requirements coming from GDPR, especially:
  - Art. 13 (information to be provided where personal data are collected from the data subject)
  - Art 14 (information to be provided where personal data have not been obtained from the data subject)
- Must be provided in country A (when obtaining patient data)
- Must be provided in country B (when accessing patient data)

# Traceability

- Each component is producing ATNA logs
- Non-repudiation assertions are produced and logged
- No content is logged by either NCP-A or NCP-B – only digests are logged in ATNA secure node

# How can IHE support GDPR implementation?

- Keep a log of who is accessing what and when
  - ATNA (Audit Trail and Node Authentication) IHE Profile is designed to record this kind of information (among other)

- Obtain and document patient consent
  - BPPC (Basic Patient Privacy Consent) and APPC (Advanced Patient Privacy Consent) IHE Profiles can be used to document a patient consent as a CDA document

Full compliance with GDPR requirements is still a work to be performed. Other profiles like IUA (Internet User Authentication) and XUA (Cross-Enterprise User Assertion) may also be useful.

# GDPR and CBeHIS

| GDPR requirement | CBeHIS answer | Comment |
|---|---|---|
| Patient Information and Consent | Patient Information Notice both in country of origin (e.g. during patient registration) and in country of care (before care) | Partly in place<br>Logistic aspects in country B to be clarified (when, language, storage, …) |
| Accountability | ATNA logs | In place |
| Non repudiation | Non repudiations assertions based on eSens specs | In place but not fully capable of dispute resolution. Specs to be enhanced and then implemented |
| Minimisation | Patient Summary specification | Content designed with and validated by healthcare professionals |
| Portability | HL7 CDA r2<br>Use of international terminologies as much as possible (revision in progress) | Patient Summary based on PCC ePrescription and eDispense based on IHE Pharmacy |

# Reference documentation

**IHE** (available on IHE Web Sites)

- White Paper «IHE perspective on the European Union GDPR» (IHE Europe, April 2018)

  https://www.ihe-europe.net/sites/default/files/2018-05/IHE-Europe-GDPR%20White%20Paper-2018.pdf

- ATNA, APPC, BCCP IHE Profiles (IHE International)

  https://www.ihe.net/resources/technical_frameworks/

**CBeHIS** (available on CEF eHDSI Web Site)

- Model Patient Information Notice
- Specifications

  https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/Specifications