Push authorization - the Whitebox model

Guido van ‘t Noordende

Guido van ‘t Noordende
Whitebox Systems Amsterdam

white box

Decentralized **push autorisation**

#how? *pull* after *push*

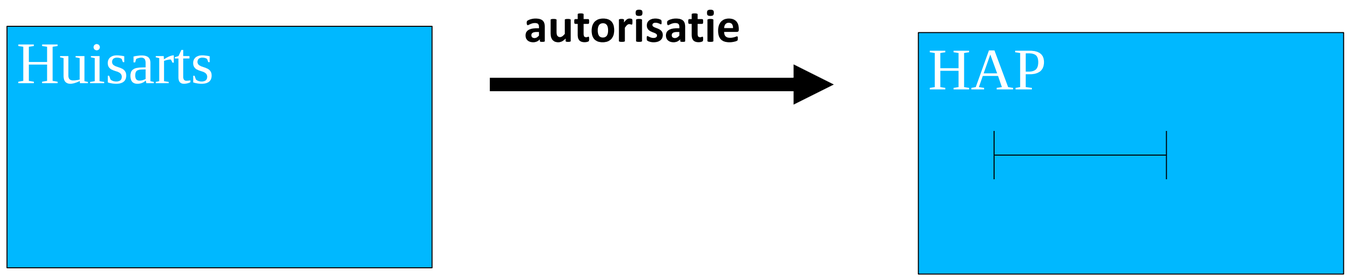
Decentrale autorisatie #principe/concept

Basisprincipe: iedere geautoriseerde partij krijgt een eigen unieke autorisatie (URL) per patient

autorisatie

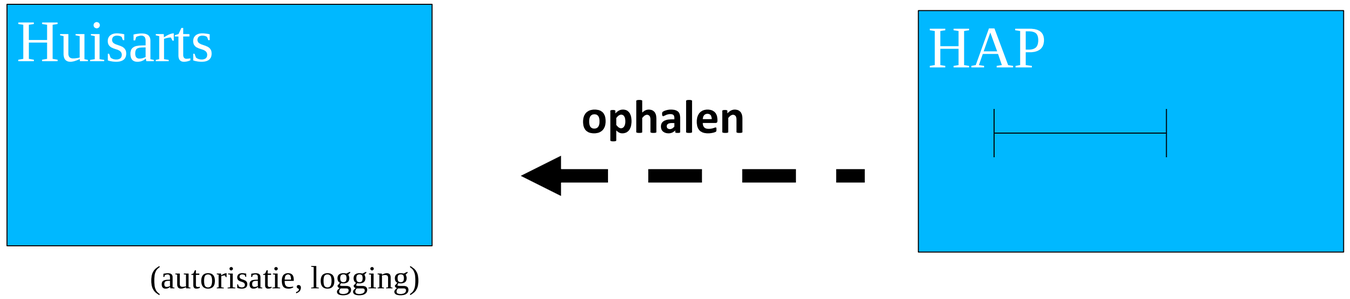
Autorisatie-URLs #technisch/schematisch

Eerste stap: autorisatie HAP



Autorisatie-URLs #schematisch

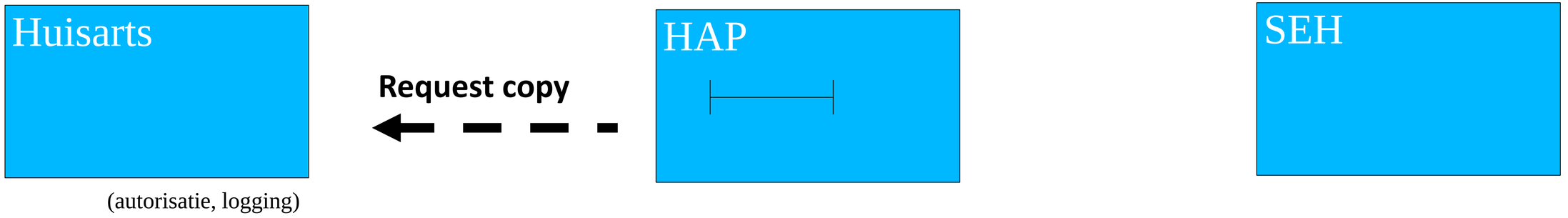
Op later moment, ophalen



(autorisatie, logging)

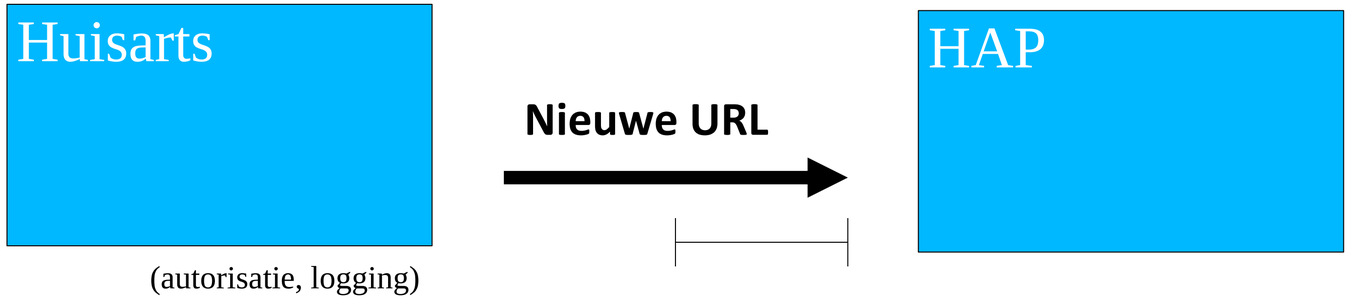
Autorisatie-URLs #schematisch

Doorautoriseren (naar SEH)



Autorisatie in ketens #principe/concept

Doorautoriseren (naar SEH)

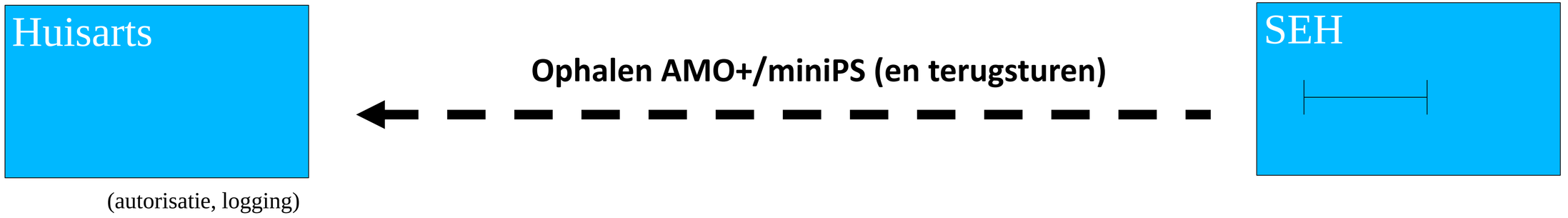


Autorisatie in ketens #principe/concept

Doorautoriseren (niet data doorkopieren!)

Autorisatie in ketens #principe/concept

Doorautoriseren (niet data doorkopieren!)



Decentrale autorisatie #principe/concept

Baisprincipe: elke partij krijgt een unieke autorisatie (url)

ophalen

Decentrale autorisatie #principe/concept

Basis: vast netwerk (vaste partners)
rond huisarts/patient

Decentrale autorisatie #principe/concept

Dynamisch uitbreidbaar
- **Soms tijdelijk**
- **Soms permanent**

Indexloos communiceren #dynamisch

Trusted partners

Indexloos communiceren #dynamisch

verwijzing

Indexloos communiceren #dynamisch

verwijzing

doorverwijzing

Indexloos communiceren #dynamisch

Trusted partners

verwijzing

doorverwijzing

recept

Afschrift (MP9!)

Terugcommuniceren

Autorisatie bij spoed #dynamische doorautorisatie

Trusted partners

24/7 availability of GP in case of emergency

Autorisatie bij spoed #dynamische doorautorisatie

Trusted partners

13245

* De technologie voor vertalen van een autorisatie URL naar een code is buiten scope voor deze presentatie

Autorisatie bij spoed #dynamische doorautorisatie

Trusted partners

13245

Autorisatie bij spoed #dynamische doorautorisatie

Trusted partners

Patient may also carry (permanent) autohrizations, or generate these using an App that is connected to the GP

456723

Autorisatie bij spoed #dynamische doorautorisatie

Trusted partners

fetch dossier

Autorisatie bij spoed #dynamische doorautorisatie

Trusted partners

Pushback communicatie naar/via eigen huisarts

verwijzing

Sharing data in an organized way (or: replacing the data broker)

(medical) research data management

white box

- Microdata often identifiable (Koot et al.)
- Pseudonymized data is considered personally identifyable

Often no transparency over the full data processing pipeline / chain

- Consent often too broad; data (re)combination often untraced
- Data brokers: mixed interests?

What to do?

- Transitive authorization and policy enforcement
- Avoid ‘copying out of sight’
- Separation of concerns

Secondary use #datamanagement

Separation of roles

Coordinating research requests

Trust link*

Research coordinating party

Secondary use #datamanagement

Separation of roles

Coordinating research requests

Trust link*

Research coordinating party

Does not process (broker) actual data

Secondary use #datamanagement

Separation of roles

Coordinating research requests

Research coordinating party

Request
(query, purpose description, description of constraints)

Research party (requires data)

Secondary use #datamanagement

Separation of roles

Validation of research request

Research coordinating party

Request
(query, purpose description, description of constraints)

Research party (requires data)

Secondary use #datamanagement

Separation of roles

Validation of research request

Research coordinating party

Query and purpose and constraint specification,

Other details like pseudonymization key may also be communicated to source system

Secondary use #datamanagement

Separation of roles

Validation of research request

Autorisation

Research coordinating party

Implements query and constraints, possibly vetted by doctor

With microdata: permission patient

Secondary use #datamanagement

Separation of roles

Validation of research request

Autorisation per pt

Research coordinating party

Secondary use #datamanagement

Separation of roles

Validation of research request

Research coordinating party

Autorisation

Researcher

Secondary use #datamanagement

The process is replicateable

Research coordinating party

Autorisation

Researcher

Secondary use #datamanagement

All sources audit (log) the requests

fetch

fetch

fetch

fetch

Researcher

Secondary use #datamanagement

Note: the computation for the researcher may actually be done in a secure container of a trusted third party (Freek's example).

This may actually be a constraint imposed by the research request coordinator

Researcher

Secondary use #datamanagement

Wrapping up

close

close

close

close

Researcher

Aggregation, ..

Result consumer

Secondary use #datamanagement

Researcher

Data cleanup.

Result consumer

Secondary use #datamanagement

Done.

Results

Privacy by design in healthcare.

white box

- **Track (audit) all data transitions** through the data processing pipeline
- **Tracking and responsibility** at the source
- **Authorize** within existing, clear and well-defined (health) worlkflows (clinical context: Wgbo)
- **Separate concerns/incentives** Separate policy specification and authorization from policy enforcement / processing
- **(Formal) query validation processes**; certification, governance

white box

Thank you

Overview of some of my current work:

https://blog.gidsopenstandaarden.nl/2020/03/Guido-van-t-Noordende-ketentransparantie-data-essentieel.html