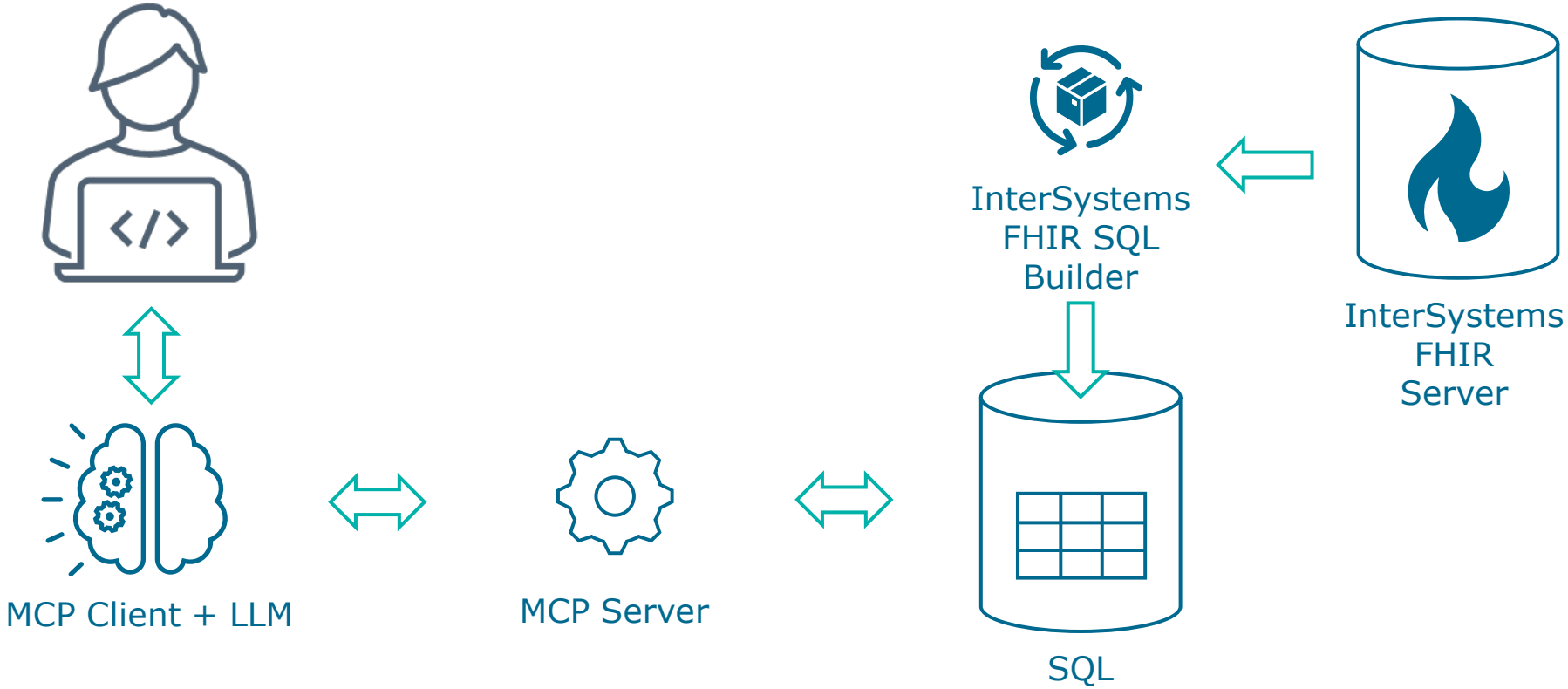
InterSystems
DACH Symposium 2026

ChatFHIR auf dem InterSystems AI Hub

Sylwester Boldt, InterSystems

Recap: Vom Chatbot zum FHIR Agent



Dr. Anna Weber: **„Wie verteilen sich unsere Diabetes-Patienten nach Geschlecht und Altersgruppe?“**

Migration auf den AI Hub

Die Anwendung bleibt gleich, die technische Verantwortung liegt jetzt in der Plattform

1. **Runtime** — IRIS-Image mit AI Hub
2. **Configuration** — MCP-Web-App, TOML, Credentials
3. **Code** — %AI.Tool-Klassen oder <Query> im ToolSet
4. **Security** — Rollen, Benutzerkontext, Policies
5. **Validation** — MCP-Calls testen, alten Container entfernen

Vorher

User

eigener

Nachher

Web Gateway (A)

```
<Query Name="GetConditionStatistics"
       Description="Return the number of patients with a condition (SNOMED code, e.g. 44054006),
                    grouped by gender and age group. Aggregated, no individual patient data."
       Arguments="SnomedCode As %String">
  SELECT Description, Gender, AgeGroup, PatientCount
  FROM ChatFHIR_Stats.ConditionStatistics
  WHERE SnomedCode = :SnomedCode ORDER BY Gender, AgeGroup
</Query>
```

(B) Identität — Verbindung

A **Am Web Gateway vorbei:** Agent-Traffic belastet den Webserver nicht.

B **Zwei Auth-Layer:** Verbindung und Identität sind getrennt. Ohne Identität pro Request keine Tools: die Basis für Governance.

Governed: Der Agent darf nur, was der User darf

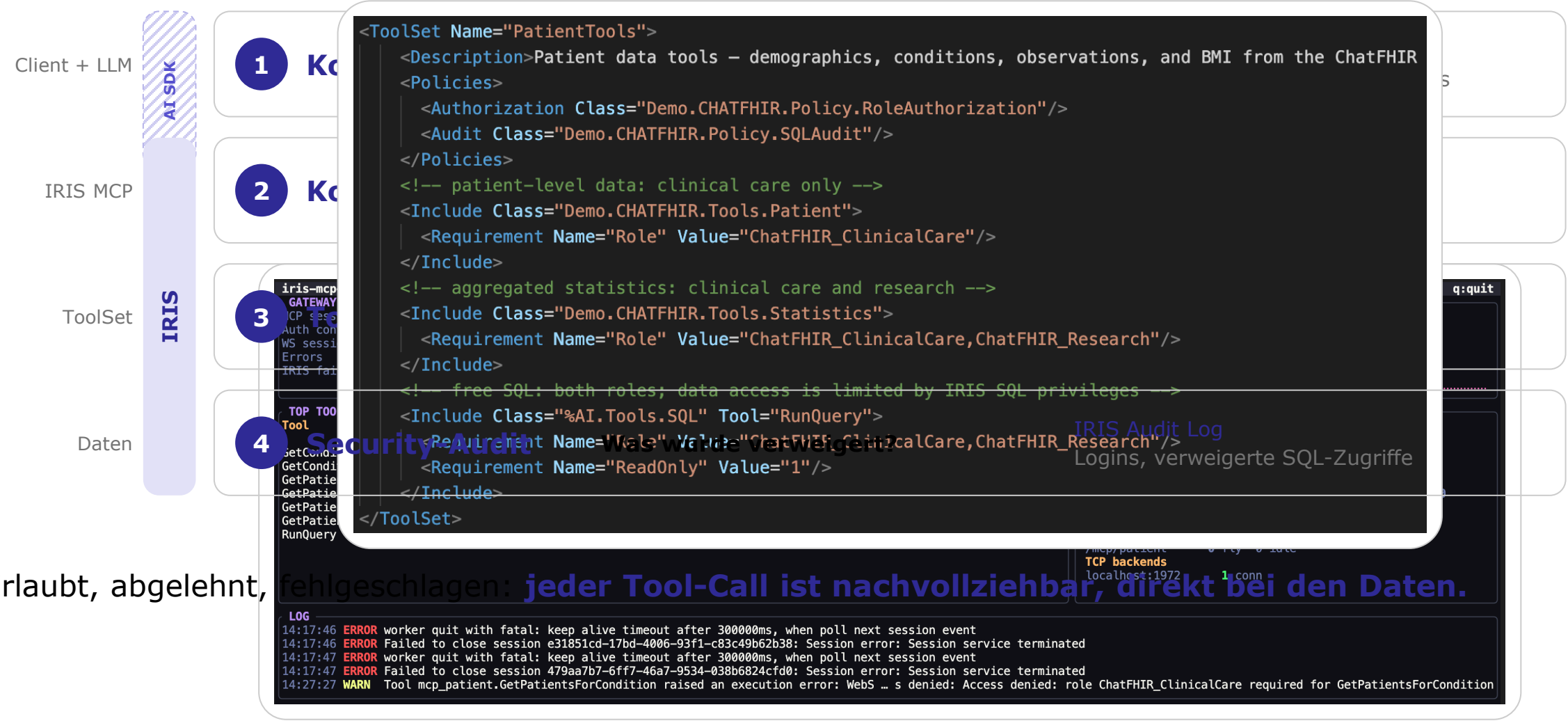
Zwei Schlösser in InterSystems IRIS: die Policy regelt die Tools, die InterSystems IRIS-Rechte regeln die Daten



Sperrt die Policy das Tool, geht die AI über SQL.
Dort hält InterSystems IRIS die Daten trotzdem zu.

Observable: Jeder Tool-Call ist nachvollziehbar

Know what your AI actually did: vier Ebenen, vom Client bis zu den Daten



Erlaubt, abgelehnt, fehlgeschlagen: **jeder Tool-Call ist nachvollziehbar, direkt bei den Daten.**

Reusable: Ein ToolSet für jeden Agenten

Governance und Audit hängen am Tool, nicht am Client



Selbst ein kompromittierter Client kommt nicht weiter: **gleiche Ablehnung, neue Audit-Zeile.**

ChatFHIR auf dem AI Hub: was bleibt

1	**Governed**	Der Agent darf **nur**, was der User darf
2	**Observable**	**Jeder** Tool-Call ist nachvollziehbar
3	**Reusable**	**Ein** ToolSet für **jeden** Agenten

Und es geht weiter: Mit der AI SDK steuert IRIS die Agenten selbst, auch über Plattformgrenzen hinweg.

With unmatched interoperability and real-time data management, InterSystems can **enable and control your AI agents.**

Danke!