— CHAPTER 20 · COMPLIANCE & AUDIT · THE HOOK

The moment the data is real, the law is watching.

Last chapter we built a working telemedicine platform — appointments, clinical documents, a searchable corpus of patient records. Compliance is not a feature you bolt on at the end. It is a property the platform must hold, continuously, on every single request. FHIR hands you two records and one gate.

— THE PROMISE

AuditEvent — who touched it · Provenance — where it came from · Consent — whether it may be touched at all

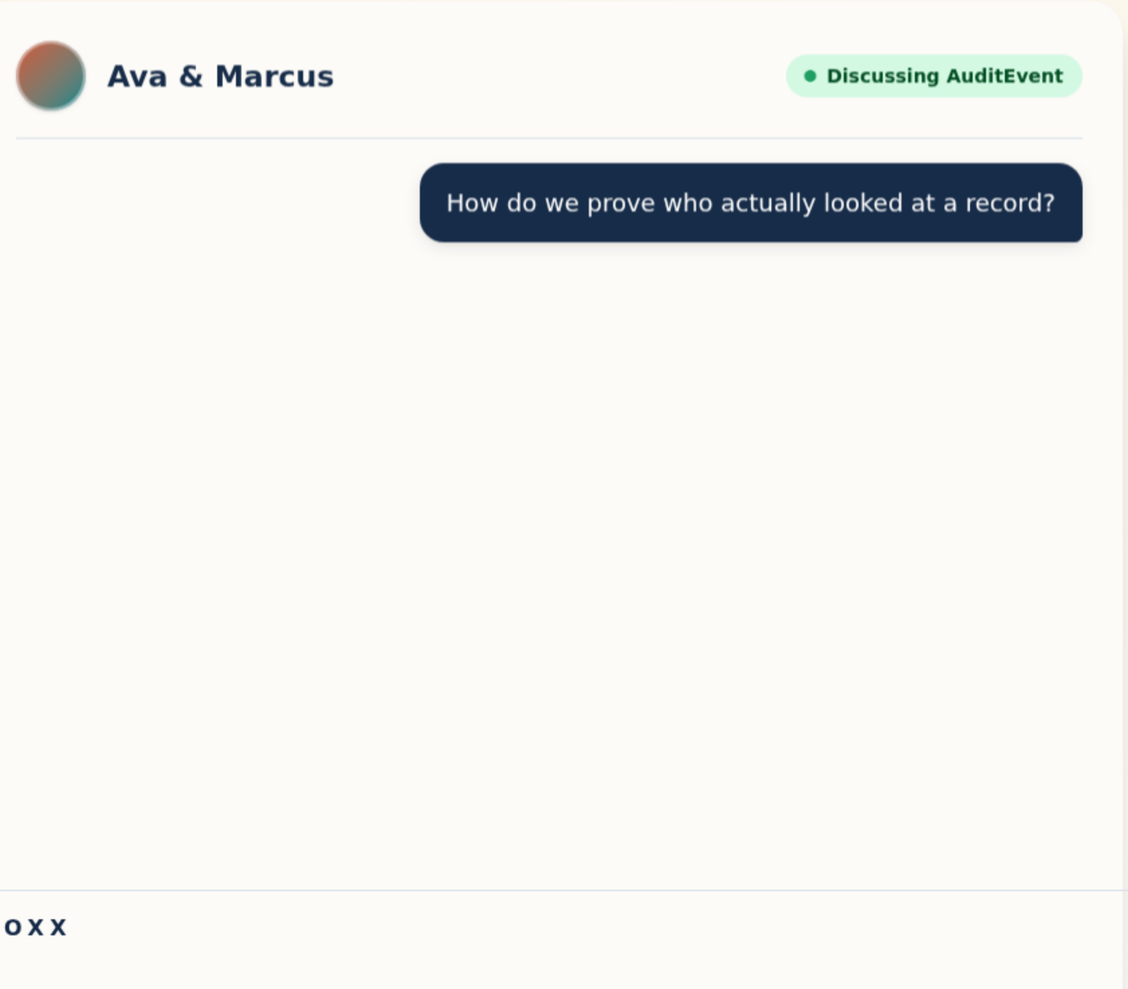
Three FHIR primitives, pulled in different directions by three regulatory regimes. The engineer's job is to hold all three at once.

What you will be able to do

— CONCEPT · AUDITEVENT — THE SECURITY AUDIT TRAIL

AuditEvent is the camera in the room.

It answers who did what, when, and where — and it is written by the responding server, the one that handled the request. It builds on the older IHE ATNA audit standard, so it is not new ground.



Core fields

What every AuditEvent records

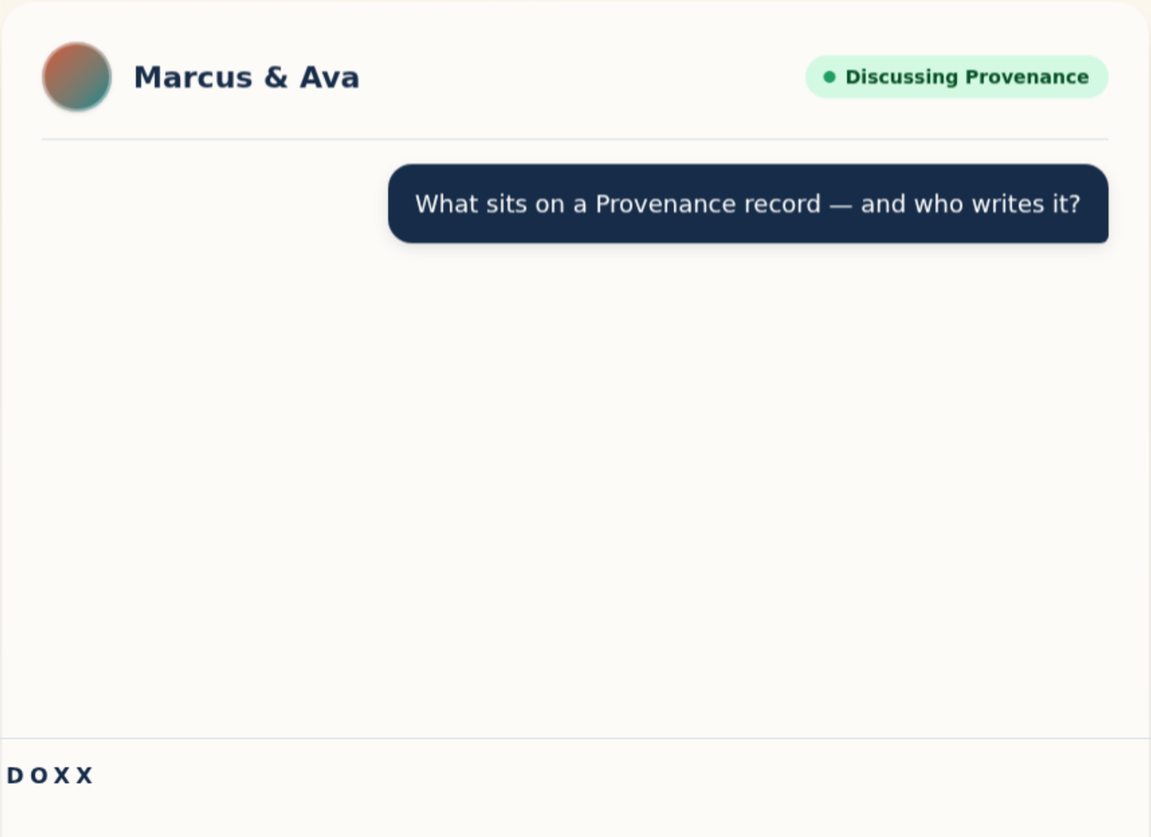
4 **outcome · entity**
success or refusal · resources touched

5 **purposeOfEvent**
why the access happened

— CONCEPT · PROVENANCE — DATA LINEAGE

Provenance answers where the data came from.

AuditEvent's sibling, and people confuse the two. Provenance is lineage — not who accessed the system, but who produced the data. It is prepared by the initiating application, the one that actually performed the create or update.



Lineage fields

What every Provenance records

4	**occurred**	optional time the activity happened
5	**signature**	non-repudiation, when needed

— REGIME 1 · HIPAA — THE AUDIT-CONTROLS MANDATE

The audit trail is not paperwork. It is a legal control.

The HIPAA Security Rule mandates audit controls — hardware, software, and procedural mechanisms that record and examine activity in any system holding electronic protected health information, ePHI. The FHIR-native answer writes those records for you.

THE MANDATE

Audit controls

Mechanisms that record and examine activity in systems holding ePHI. A requirement of the HIPAA Security Rule.

THE RESOURCE

AuditEvent

The FHIR-native record of who did what, when, and where — the exact shape the Rule asks for.

THE MECHANISM

Emit-on-access

An interceptor that emits one AuditEvent on every read and every write. The records write themselves.

ON TOP

Retention · tamper-evidence

Operational layers you add over the resource — the spec already gives you the record itself.

No audit, no compliance

AuditEvent + emit-on-access interceptor satisfies the Security Rule

— REGIME 2 · GDPR — ACCESS VS ERASURE

Two articles. One easy. One collides with the audit trail.

Make the data unreadable, without destroying the proof that it existed. That is the heart of the tension between a patient's right to be forgotten and an append-only audit and Provenance model.

— ARTICLE 15 · RIGHT OF ACCESS

Maps cleanly to FHIR

The right of access lands directly on a FHIR read and the $everything operation. The patient asks, you return their record. Easy.

- read + $everything

— ARTICLE 17 · RIGHT TO ERASURE

Collides head-on

Erasure conflicts with append-only audit and Provenance, and with clinical-record retention duties. The pattern is logical-delete or de-identification — not a physical purge.

- de-identify · preserve the trail

- Audit logs are a lawful-basis exception · clinical safety often overrides erasure

— REGIME 3 · EU AI ACT — HIGH-RISK CLINICAL AI

The audit story and the AI story are the same story.

The EU AI Act classifies AI used in medical devices and clinical decision-making as high-risk — and high-risk triggers real duties. The LLM agent from Chapter 18, reading and writing FHIR over MCP, is not exempt: if it influences a clinical decision, it can fall squarely in scope.

DUTY

Logging

AuditEvent and Provenance become the technical evidence trail the Act's logging mandate demands.

DUTY

Human oversight

A person must remain able to intervene in decisions the system influences.

DUTY

Transparency

Users must know an AI system is in the loop and how it reaches its outputs.

DUTY

Risk management

A continuous process across the system's lifecycle, not a one-time check.

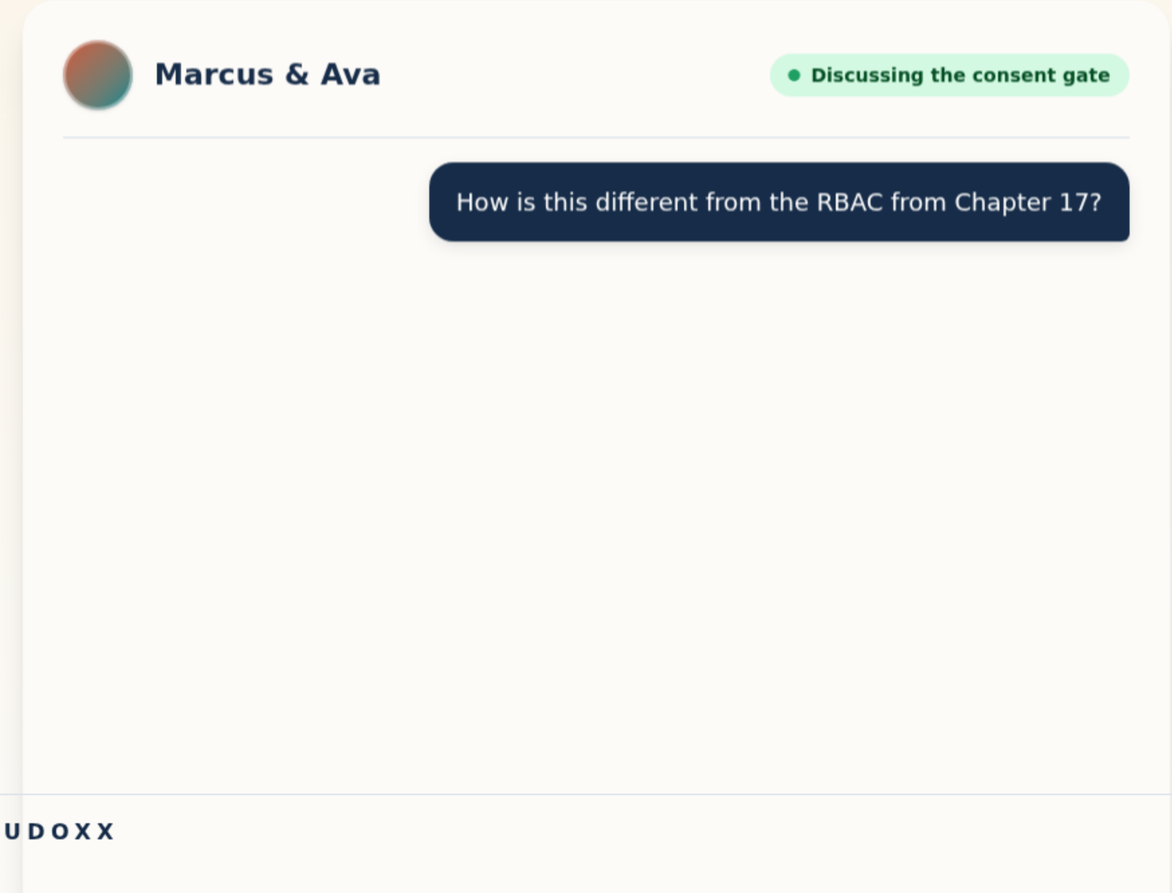
Phased — dates still settling

- Obligations phased broadly through twenty twenty-five to twenty twenty-seven
- High-risk applies broadly from around twenty twenty-six
- Ch 18 FHIR-over-MCP agents land in scope

— FRAMEWORK ANCHOR · CONSENTINTERCEPTOR 403-ABORT

Deny-by-default. The patient's own voice can override a valid role.

Audit tells us who looked — consent decides who may look at all. A Consent resource records a patient's policy: permit or deny, with a scope, a provision, the actor, the action, and the purpose.



The decision

Evaluated at the request seam, before storage

4 **Permit → storage runs**
the request proceeds

5 **Deny → abort 403**
short-circuit before storage

— SYNTHESIS · ONE REQUEST, END TO END

Permit or deny, the camera never stops recording.

Follow a single incoming read across every gate. Both paths leave a trace — a refused access is itself audit-worthy.

Ava & Marcus · Tracing one request

Walk it through — what happens if both gates pass, and what happens if consent denies?

The whole topic, one canvas

From incoming read to recorded outcome

4 **PERMIT → AuditEvent + Provenance**
storage runs · who/what/when · lineage on writes

5 **DENY → 403 · AuditEvent still logged**
the denied attempt is recorded too

— RECAP & BRIDGE · TRY IT YOURSELF

Two records, two questions — read them side by side.

Put a sample AuditEvent and a sample Provenance next to each other, label the fields, and say in one sentence which question each answers.

— AUDITEVENT · WHO TOUCHED THE SYSTEM

type · agent · source · entity · outcome

The security audit trail — who did what, when, and where. Written by the responding server.

— PROVENANCE · WHO PRODUCED THE DATA

target · agent · entity · activity

The data-lineage record — where this resource came from. Prepared by the initiating application.

Recap

- AuditEvent
- Provenance
- HIPAA audit mandate
- GDPR access vs erasure
- EU AI Act high-risk
- ConsentInterceptor 403