5.1 Approach to Auditing Data Access

Daniel Mellen – Accenture Security

Tuesday October 17th, 2006
10:00am – 11:15am
Salon D/E

5.1 Approaches to Auditing Data Access – Context

Key Words:

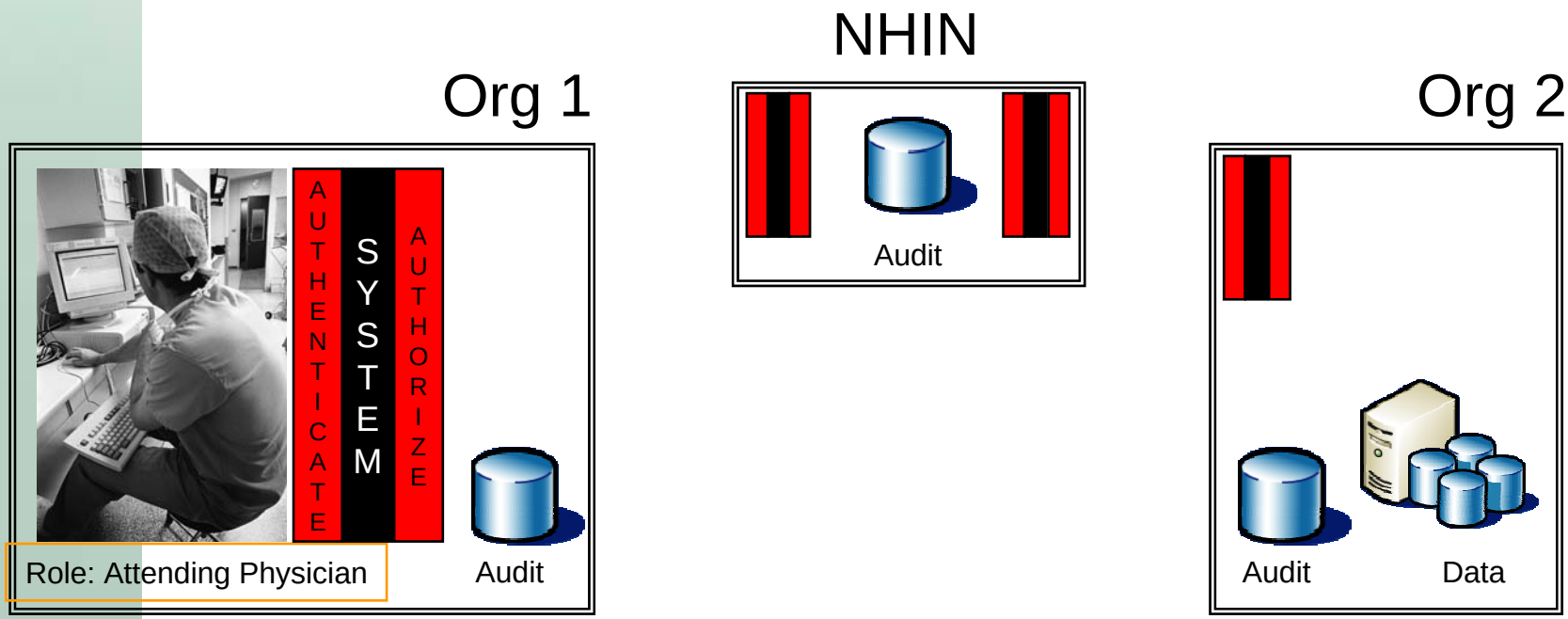
role based access controls

incoming access

outgoing requests

what data

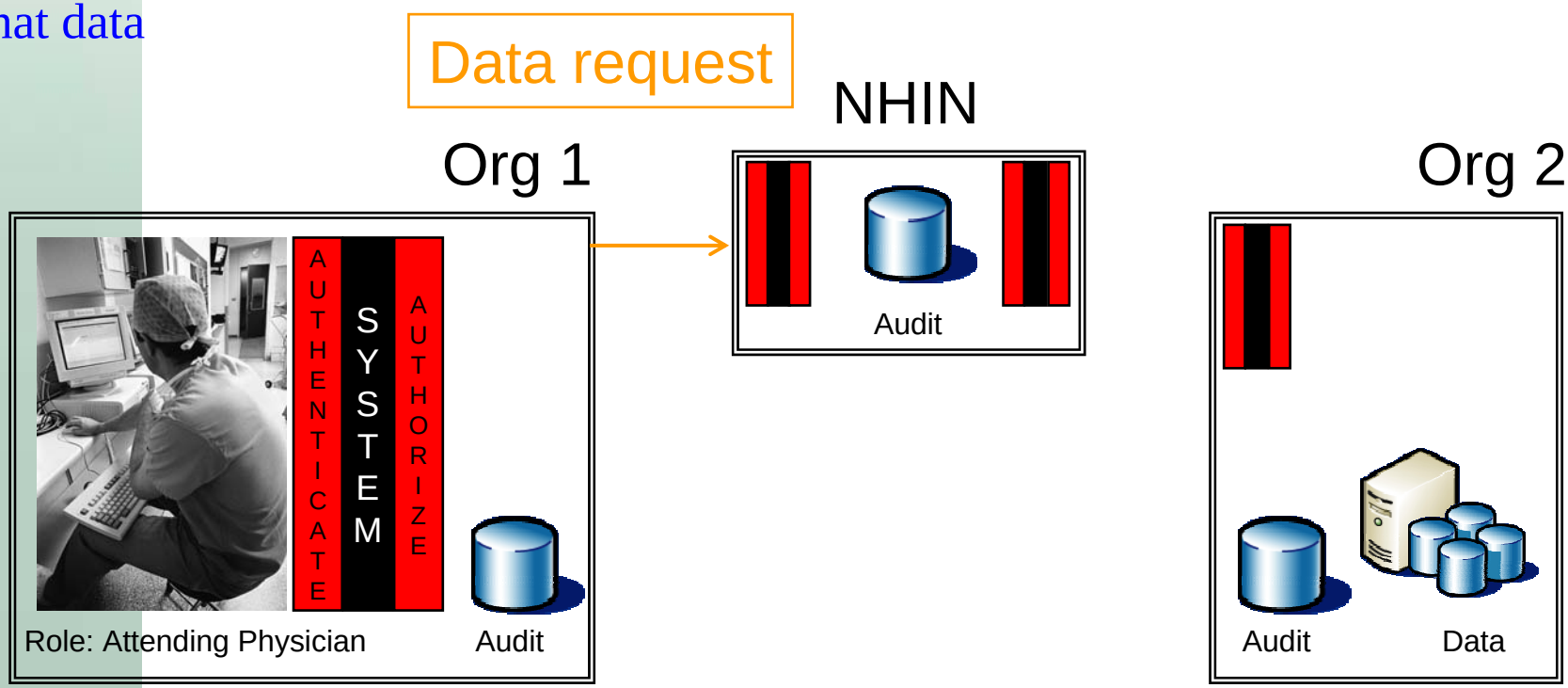
Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:
role based access controls
incoming access
outgoing requests
what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:

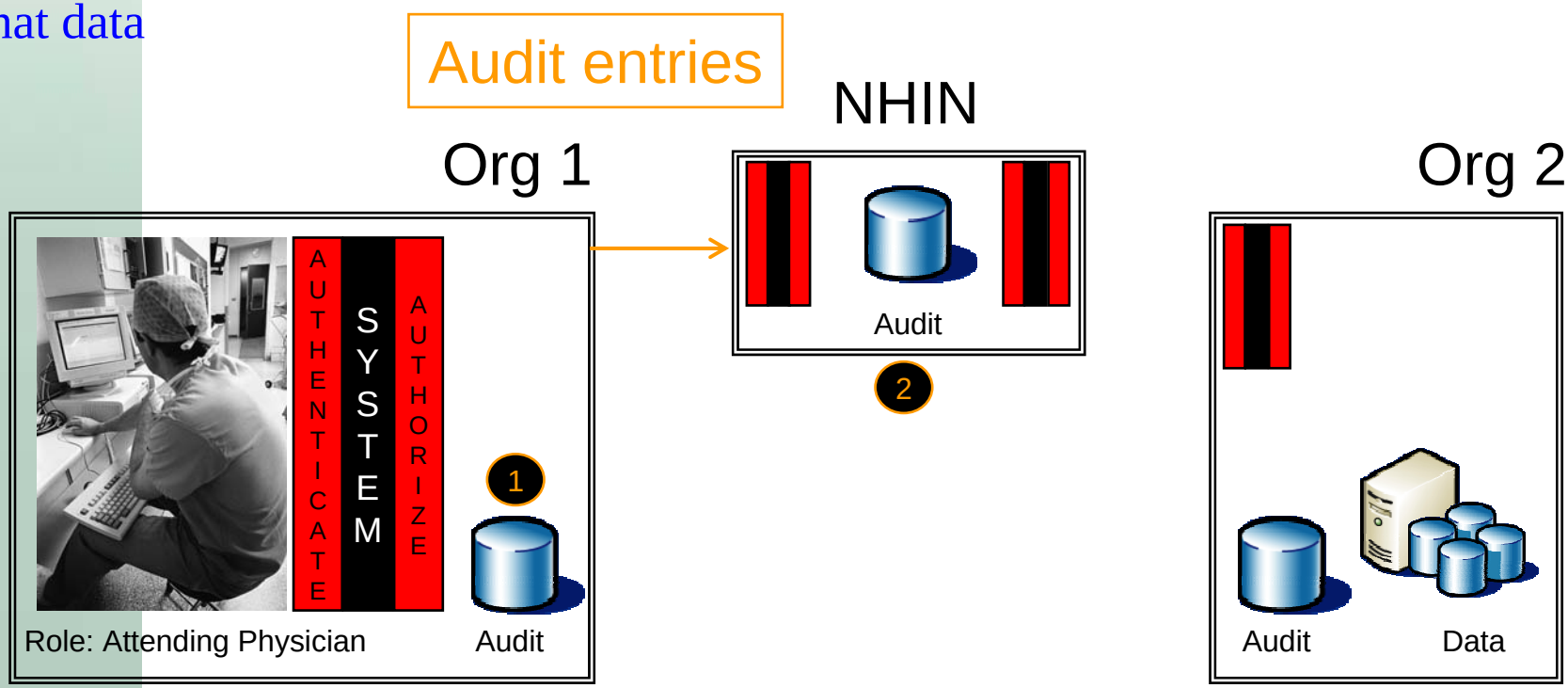
role based access controls

incoming access 2

outgoing requests 1

what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:

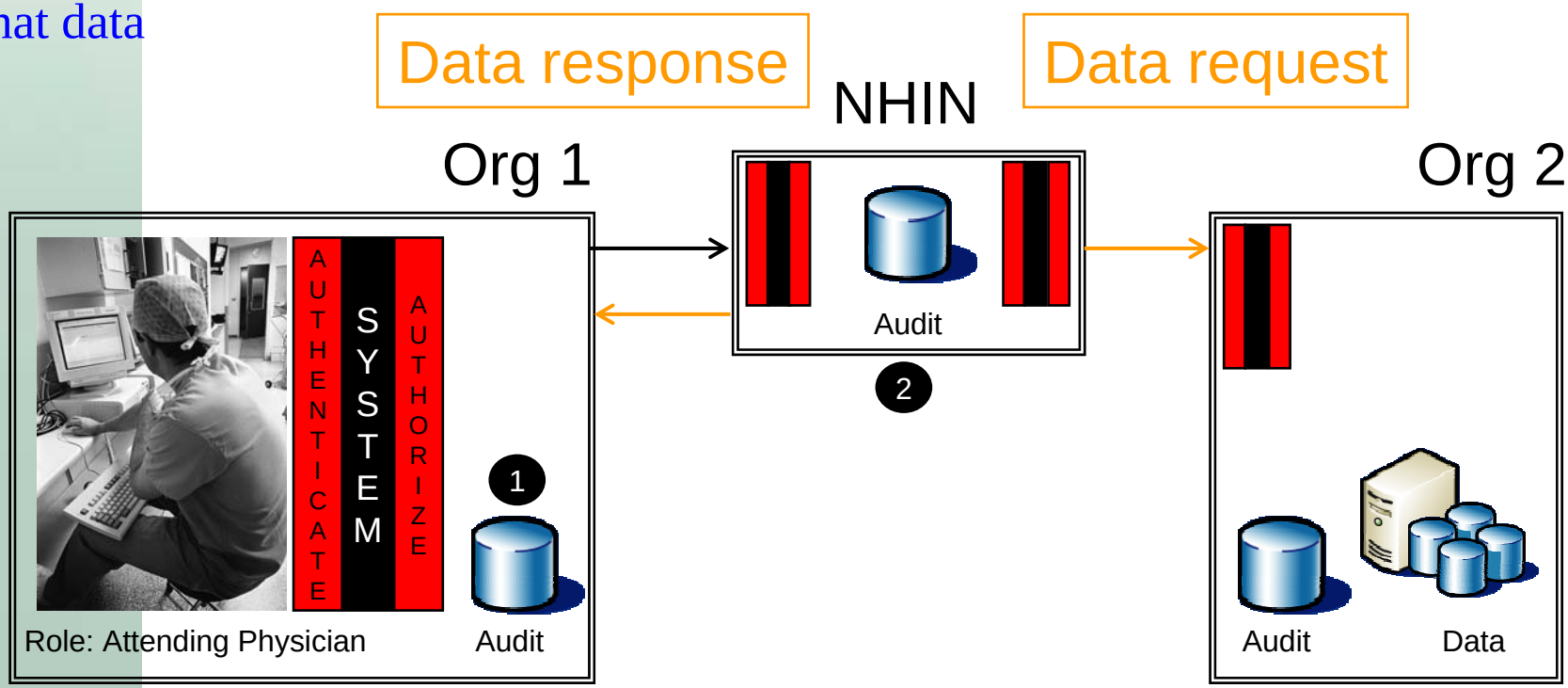
role based access controls

incoming access 2

outgoing requests 1

what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:

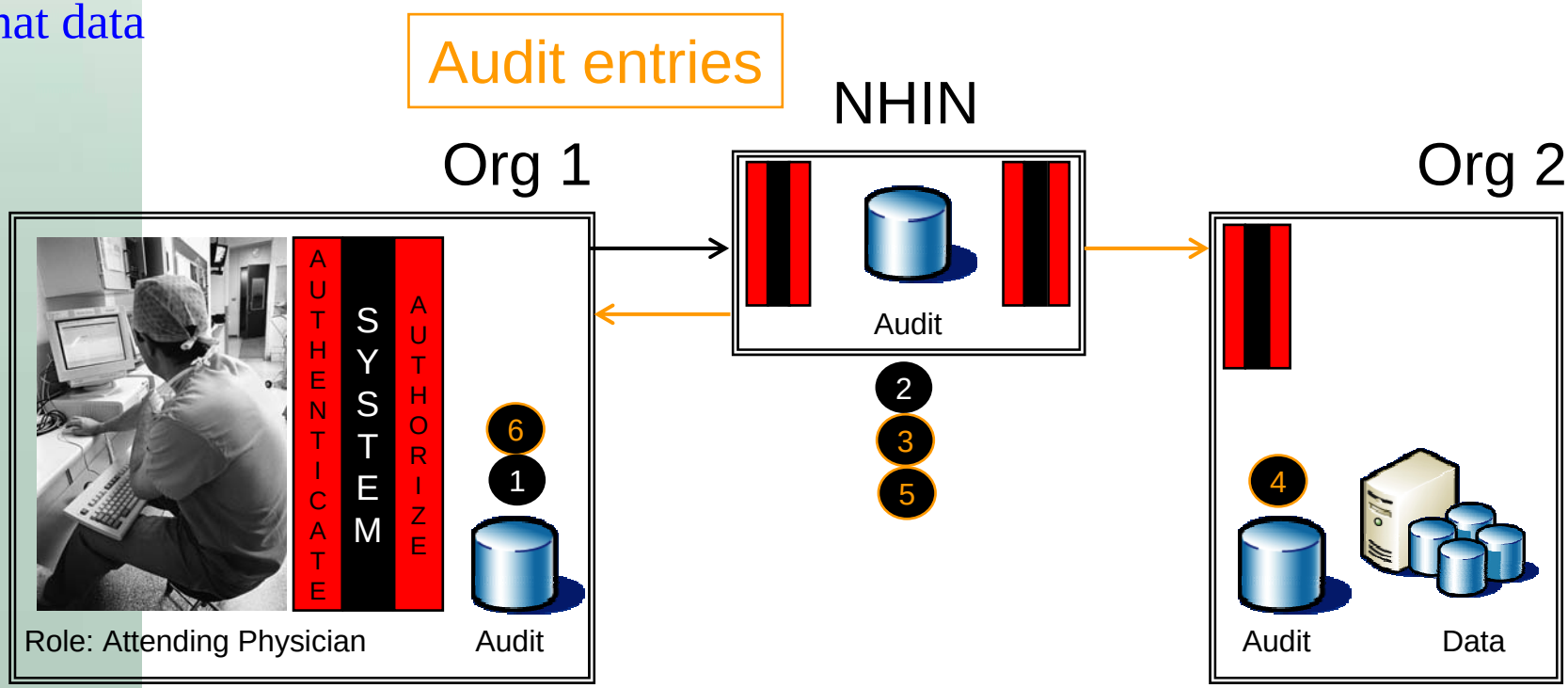
role based access controls

incoming access 2 4 6

outgoing requests 1 3 5

what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:

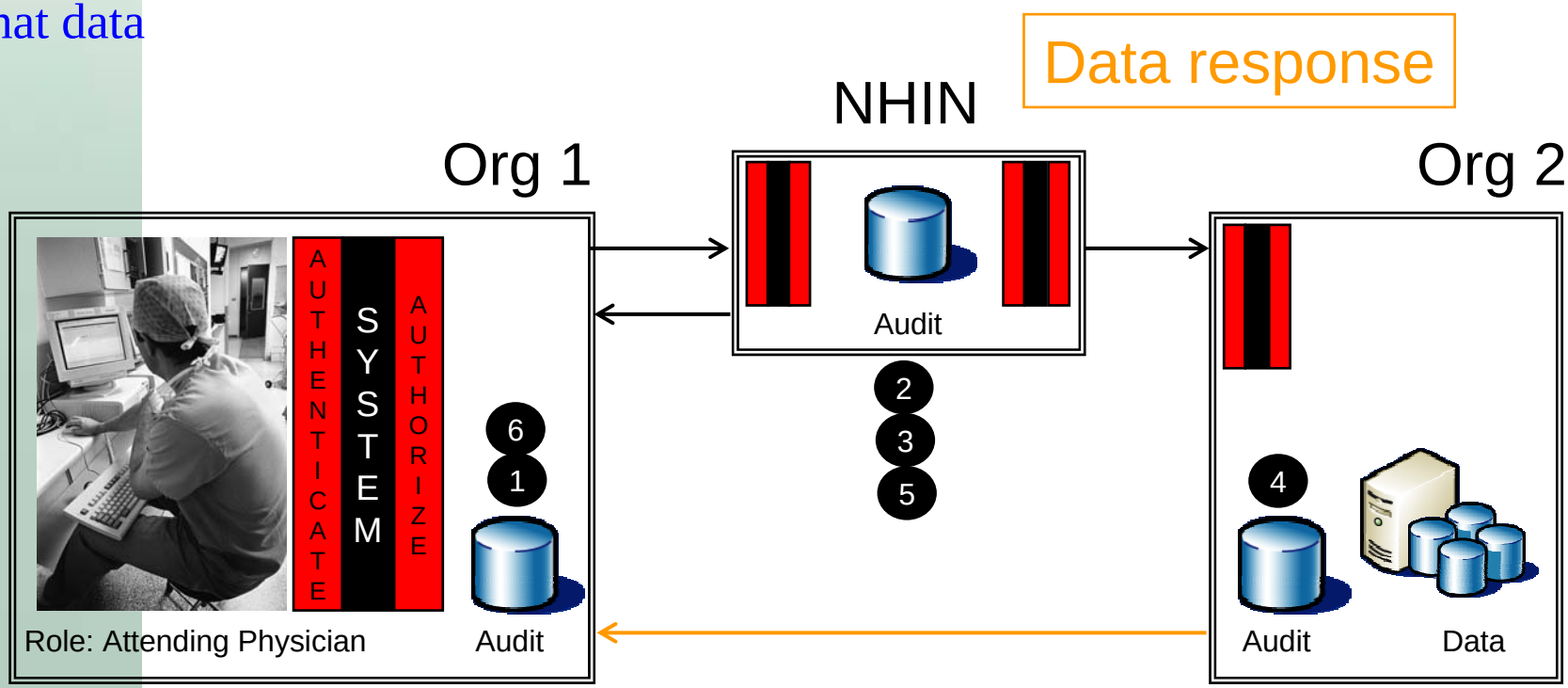
role based access controls

incoming access 2 4 6

outgoing requests 1 3 5

what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:

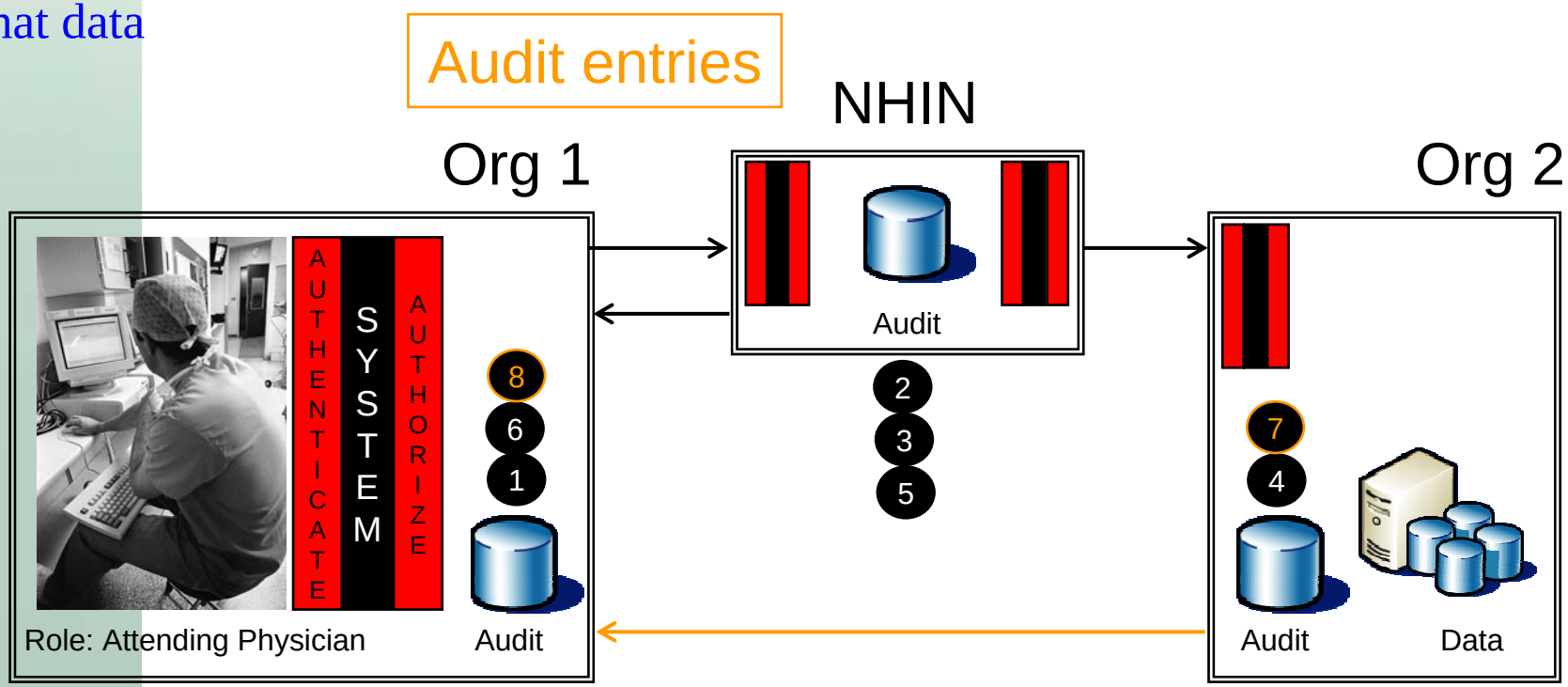
role based access controls

incoming access 2 4 6 8

outgoing requests 1 3 5 7

what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Context

Key Words:

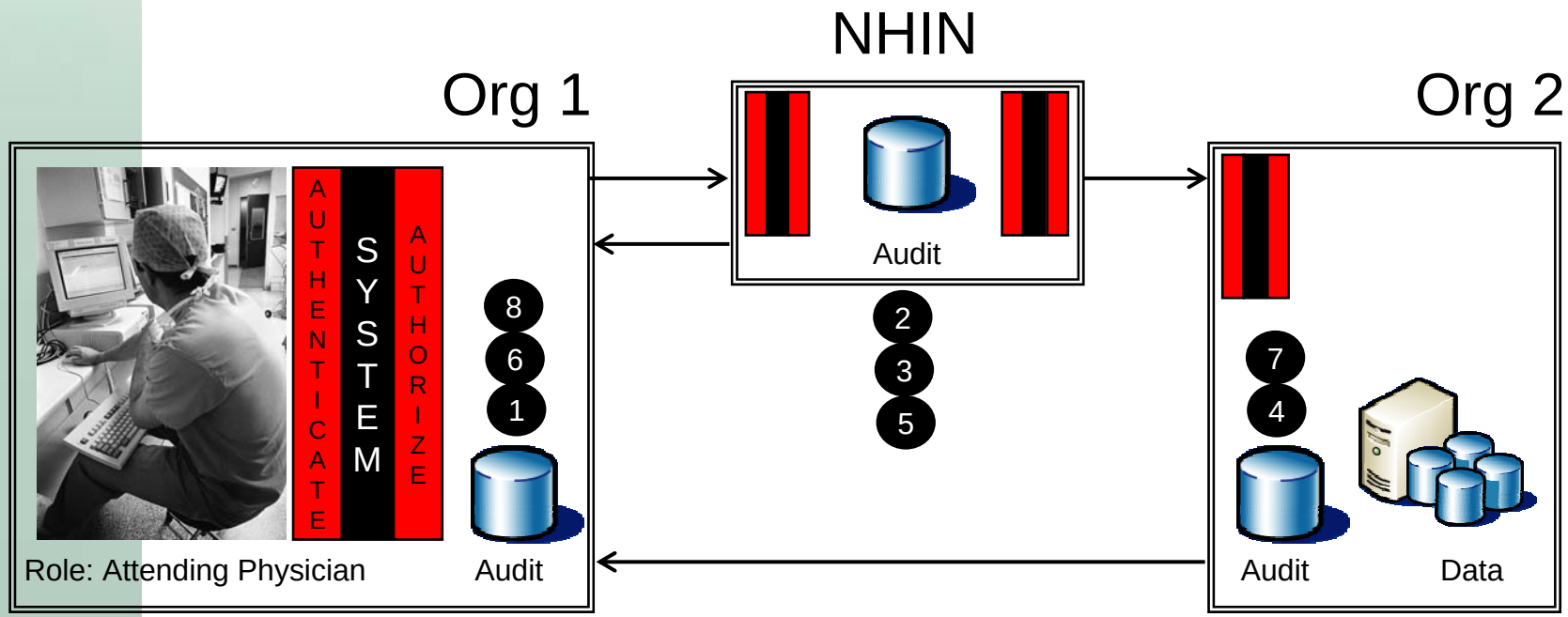
role based access controls

incoming access 2 4 6 8

outgoing requests 1 3 5 7

what data

Simple Transaction: Physician requests and retrieves patient data from remote organization.



5.1 Approaches to Auditing Data Access – Issue #1

• Types of data that need to be included in messages in order to support the audit activities of entities involved in the data exchange process.

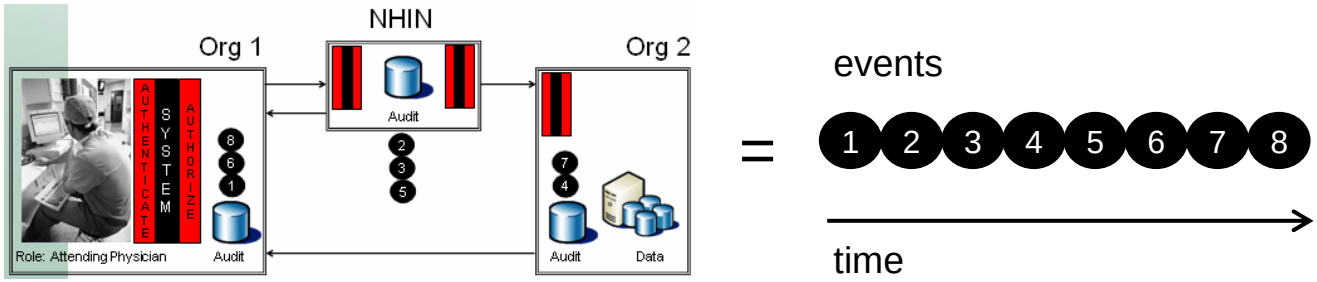
Minimum data set:
- Date and Time - Origin of authentication technique - Type of event
- Outcome of the event - Credential of the person or system
- Role of person or system - Identifier of targeted resource
- Type of action (read, update, delete, create) - Summary data
- DNS/IP/MAC address - PKI Certificate - Verification hash

- **Pros**
- **Consistent audit language**
- **Enables aggregation / sharing**
- **Reactive accountability**
- **Eases cross-entity investigations**

- **Cons**
- **Requires system integration / modification**
- **Requires additional processing & storage**
- **Introduces complexity into messaging**

5.1 Approaches to Auditing Data Access – Issue #2

• Needs to connect audit information to create a coordinated view across multiple settings.



- **Pros**
- **End to end transaction visibility**
- **Accountability across multiple settings**
- **Value added trending / predictive analysis**

- **Cons**
- **Requires multiple organization cooperation**
- **Lack of control over released data**
- **Implied participant trust**
- **Aggregation / Analysis requires more effort**

5.1 Approaches to Auditing Data Access – Issue #3

- Alerting needs for auditable events.

- **Pros**
- **Decreases potential for damage / disclosure**
- **Establishes a baseline threshold for event types**
- **Increases automation and time to discovery**
- **Focuses attention to system / user behavior**
- **Initiates trending activity**
- **Establishes communication protocol**

- **Cons**
- **Increases effort beyond current state**
  - Resources +
  - Technology +
  - O & M +
  - = Cost ($)
- **Requires consensus agreement on thresholds**
- **Introduces potential for false-positives and desensitization**