TIHI/ TID

Security Mediation

To Protect Healthcare Information Privacy in Collaborative Settings

Gio Wiederhold, PI, Michel Bilello, James Z. Wang.

past: **Jahnavi Akella, Andrea Chavez, Chris Donahue, Vatsala Sarathy, Latanya Sweeney, Yan Tan.**

Stanford University

TIHI, SAW support under subcontract to **SRI International**

TID supported under NSF Digital Libraries II

Overview

Security and Privacy when Collaborating

- **Background and Current State**
- **Unaddressed Problem**
- **Security Mediator Solution**
- **Examples including prior work**
- **Conclusion**

Security: protection and assurance

Crucial progress in protection is being made:

Remote Transmission

Authentication

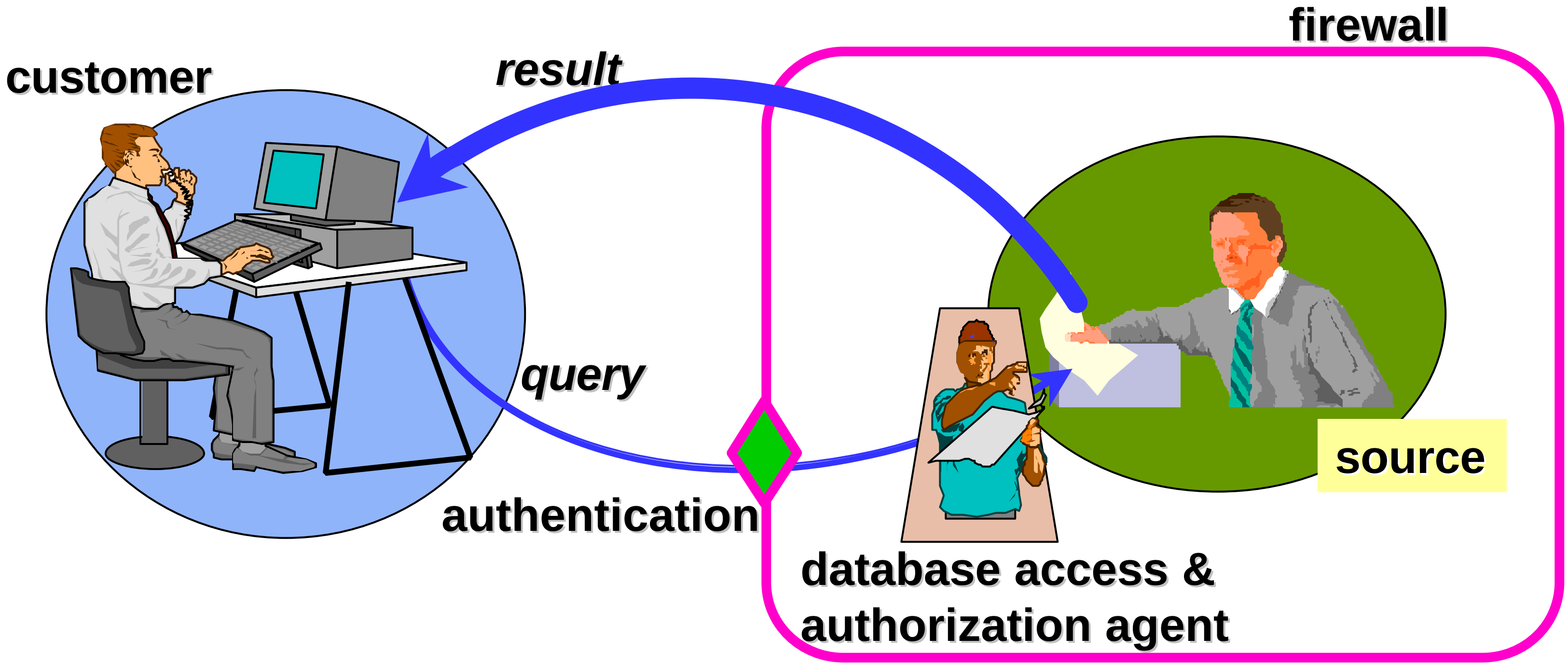
Firewalls around domains

protect against enemies.

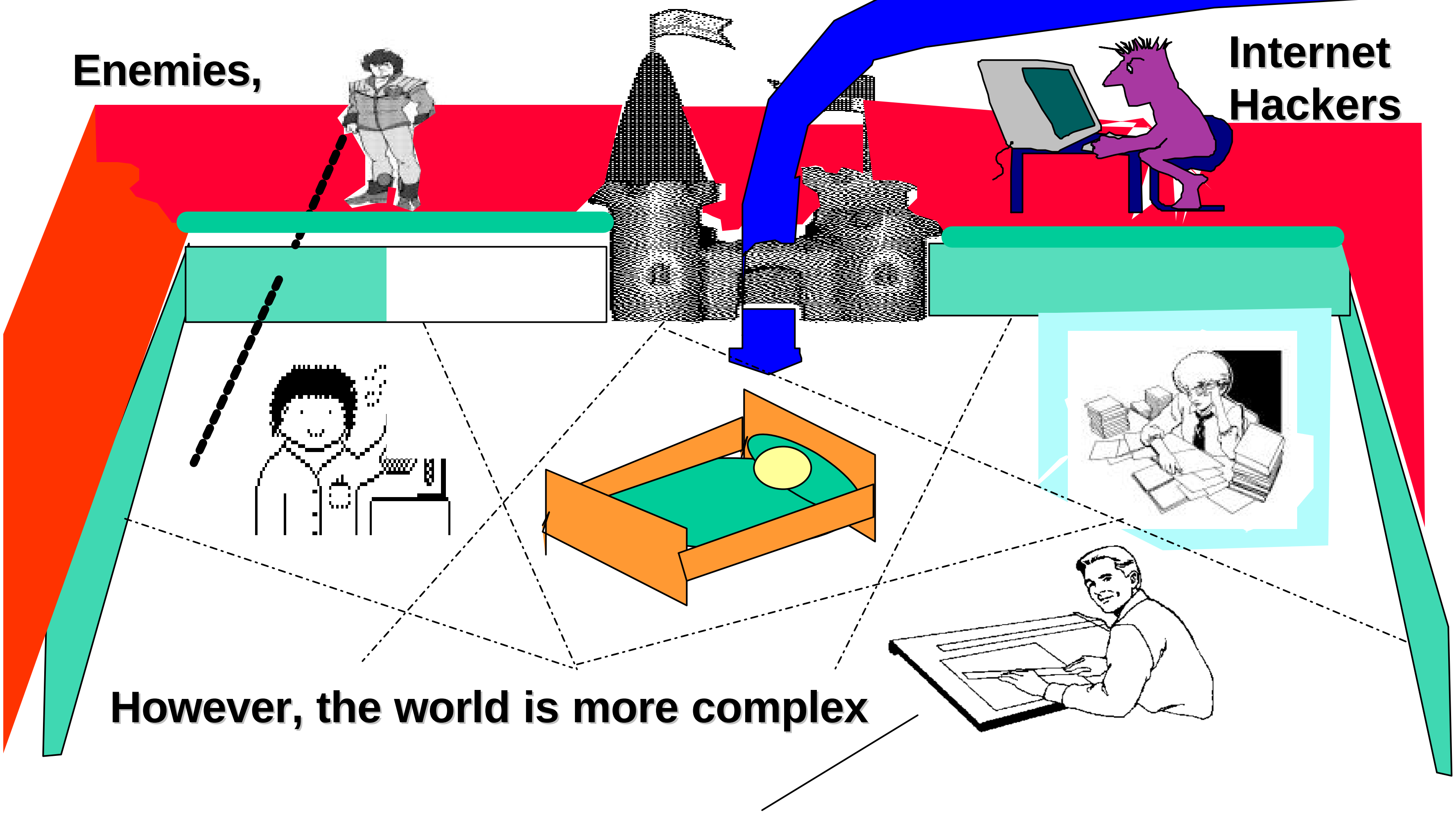
Much research based on Cryptography

Dominant approach

- Authenticate Customer
- Validate query against database schema
- If both ok, process query and ship results

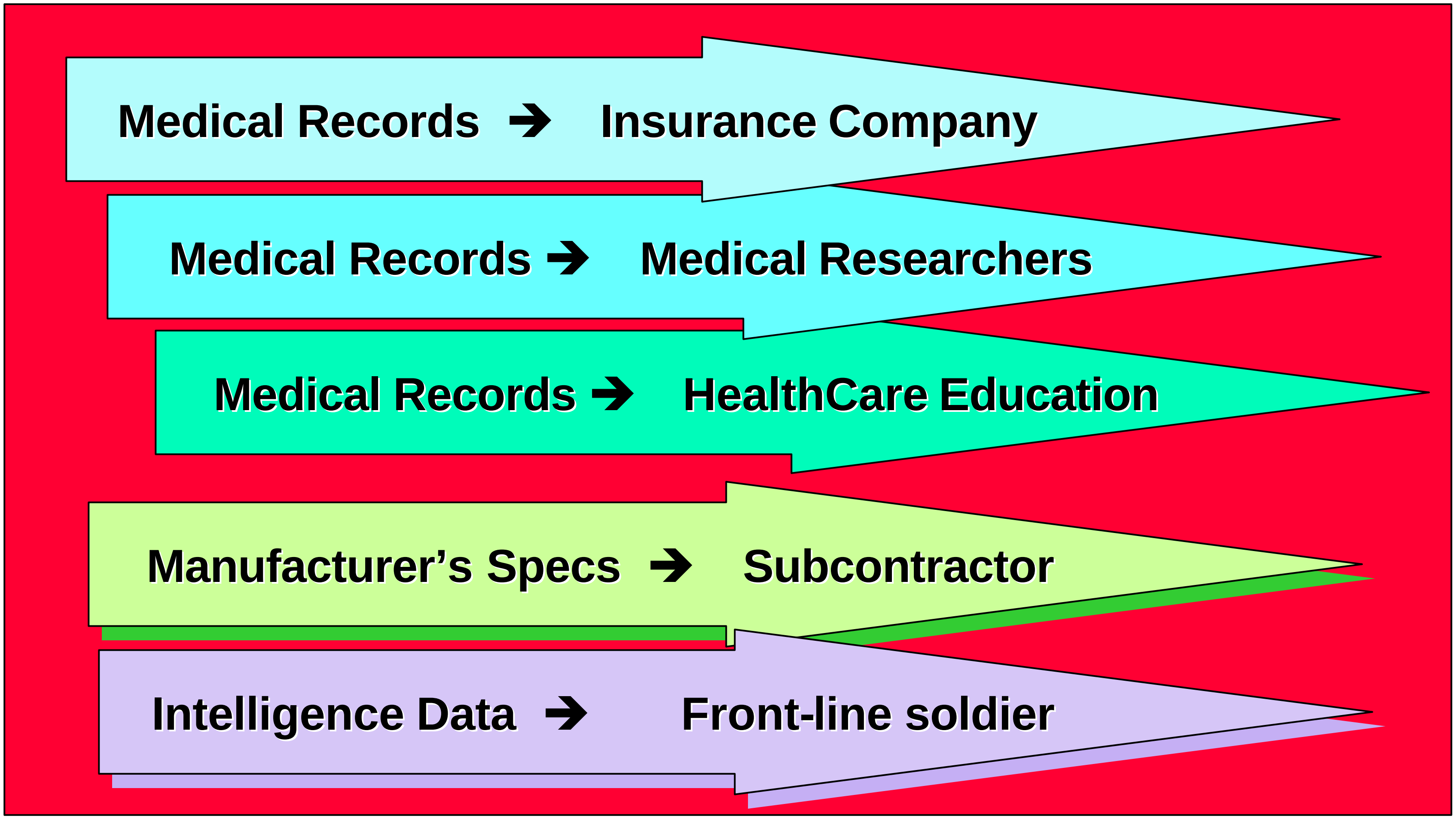


Simple View of Protection: Prohibit access .



However, the world is more complex

Collaboration Needs:



Medical Records → Insurance Company

Medical Records → Medical Researchers

Medical Records → HealthCare Education

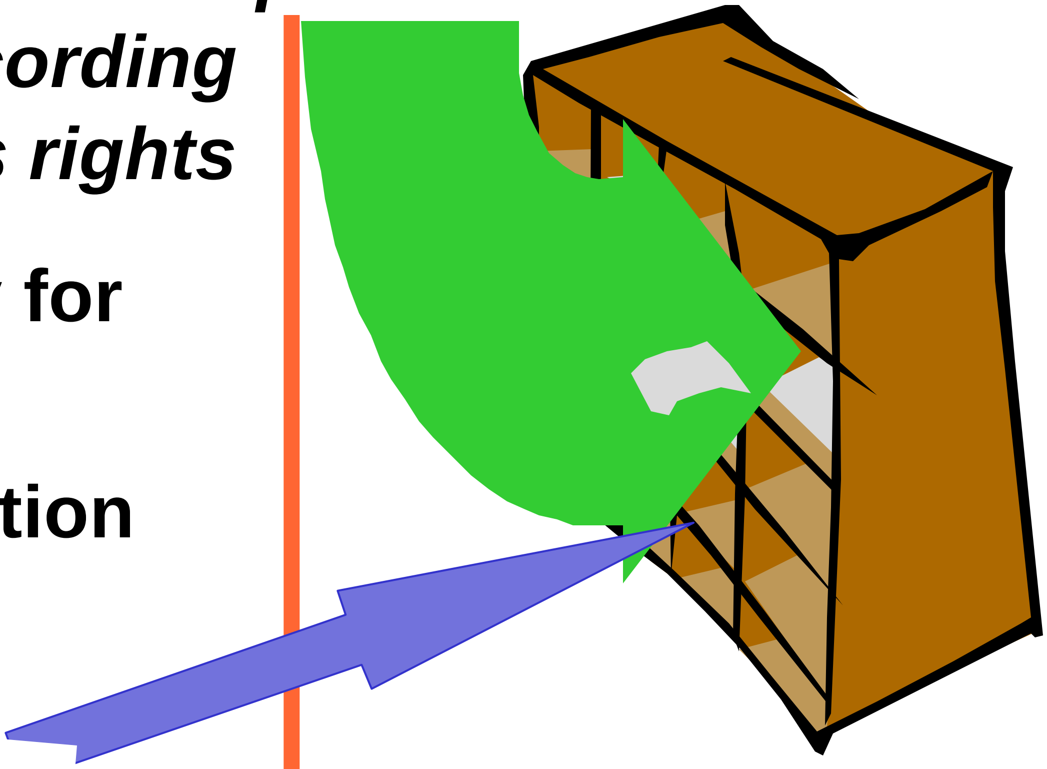
Manufacturer’s Specs → Subcontractor

Intelligence Data → Front-line soldier

False Assumption

Data in the files of an enterprise
are organized according
to external access rights

Inefficient and risky for
an enterprise
which uses information
mainly internally
and then
must serve external needs



Some Failure modes

Collaborator has legitimate access

- **Unintentionally obtains wrong data**
- **Can gain broader access than intended**

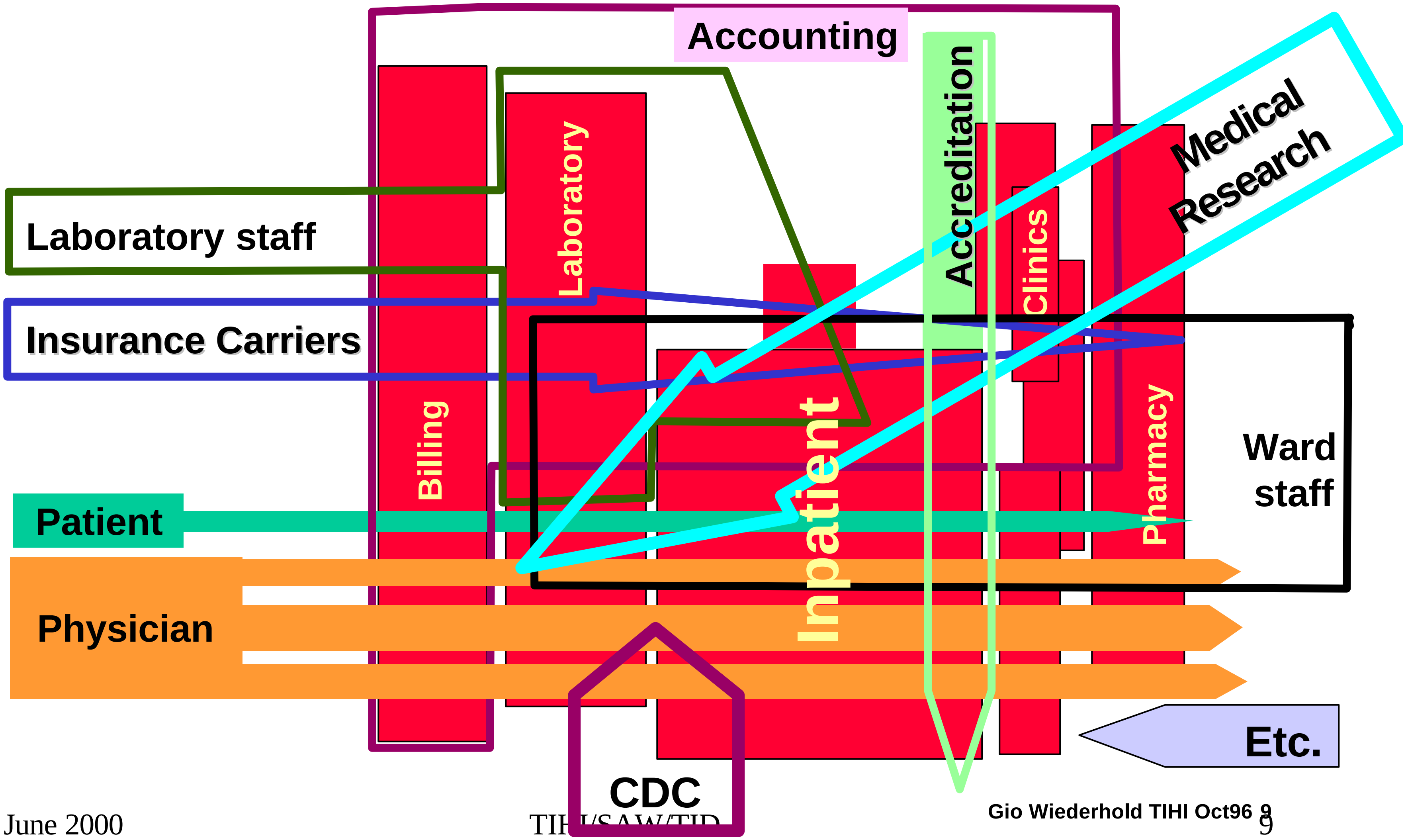
Internal user ships improper data out

- **Fails to understand release constraints**

- ***Coverage of releasable and non-releasable data overlaps***
- ***Some data are misfiled***
- ***Anonymity process fails***
  (should not separate IDs)
- ***Data replaced***
  (credit card nos instead of MP3)

- ***Backup to insecure site***
- ***(Deutsch)***
- ***Shows friend neat stuff***
- ***(Los Alamos scientist?)***

Access Patterns versus Data:



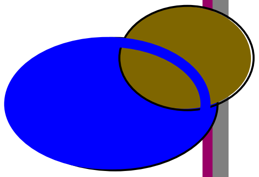
Gio Wiederhold TIHI Oct96 9

Expected Problems

Query do not specify object precisely

Relevant history for low-weight births

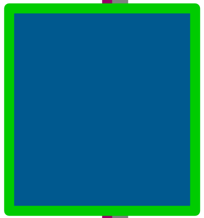
(helpful database gets extra stuff)



Objects (*N*) are not organized according to all possible access classifications (*a*) = (*N^a*)

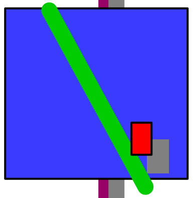
Nursing hierarchy by bed and ward

Infectious disease hierarchy by risk



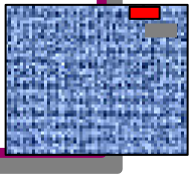
Some objects cover multiple classes

Patient with stroke and HIV

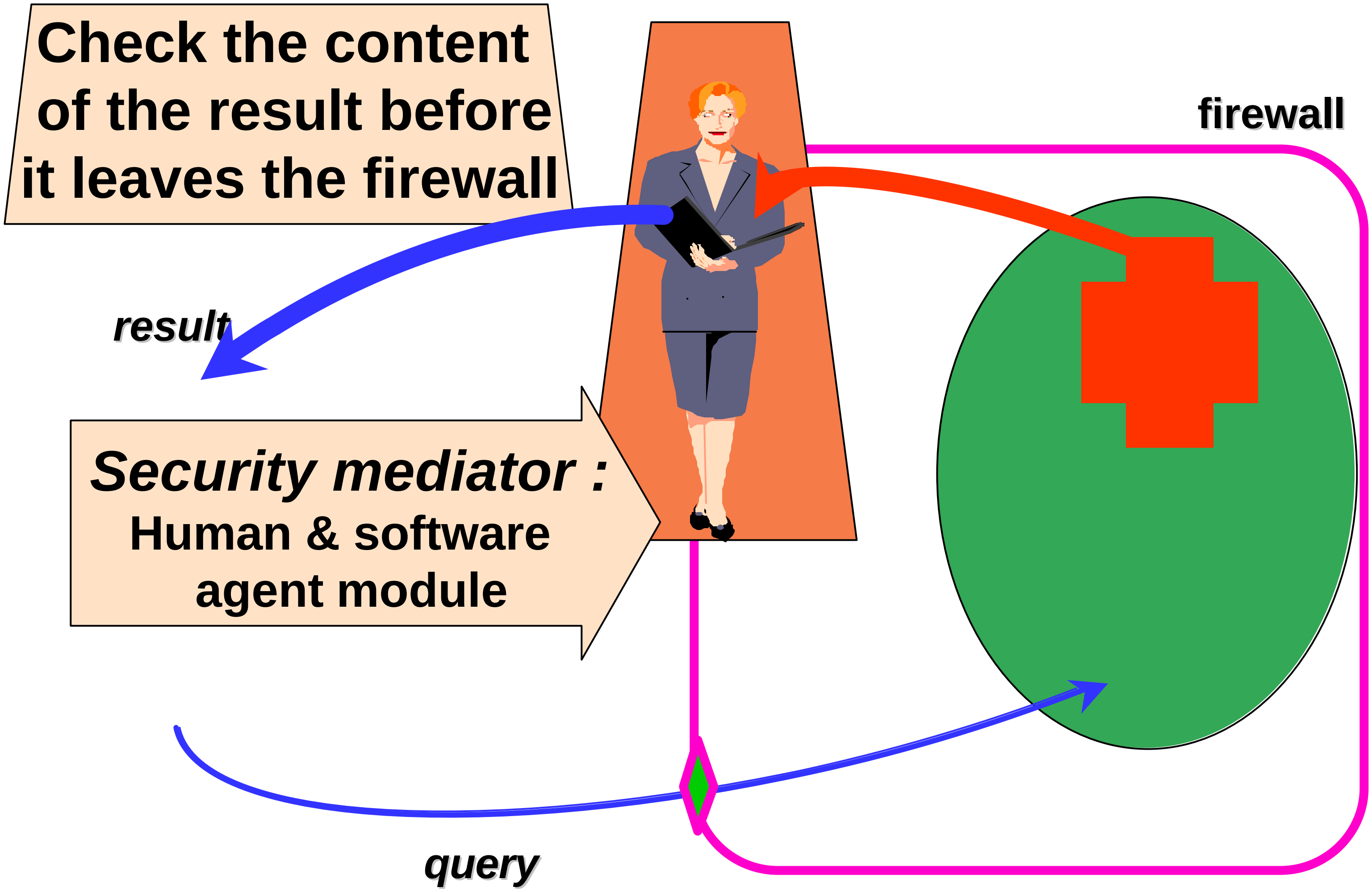


Some objects are misfiled (happens easily to others), costly/impossible to guarantee avoidance

Psychiatric data in patient with alcoholism



Securing the Gap



Check the content of the result before it leaves the firewall

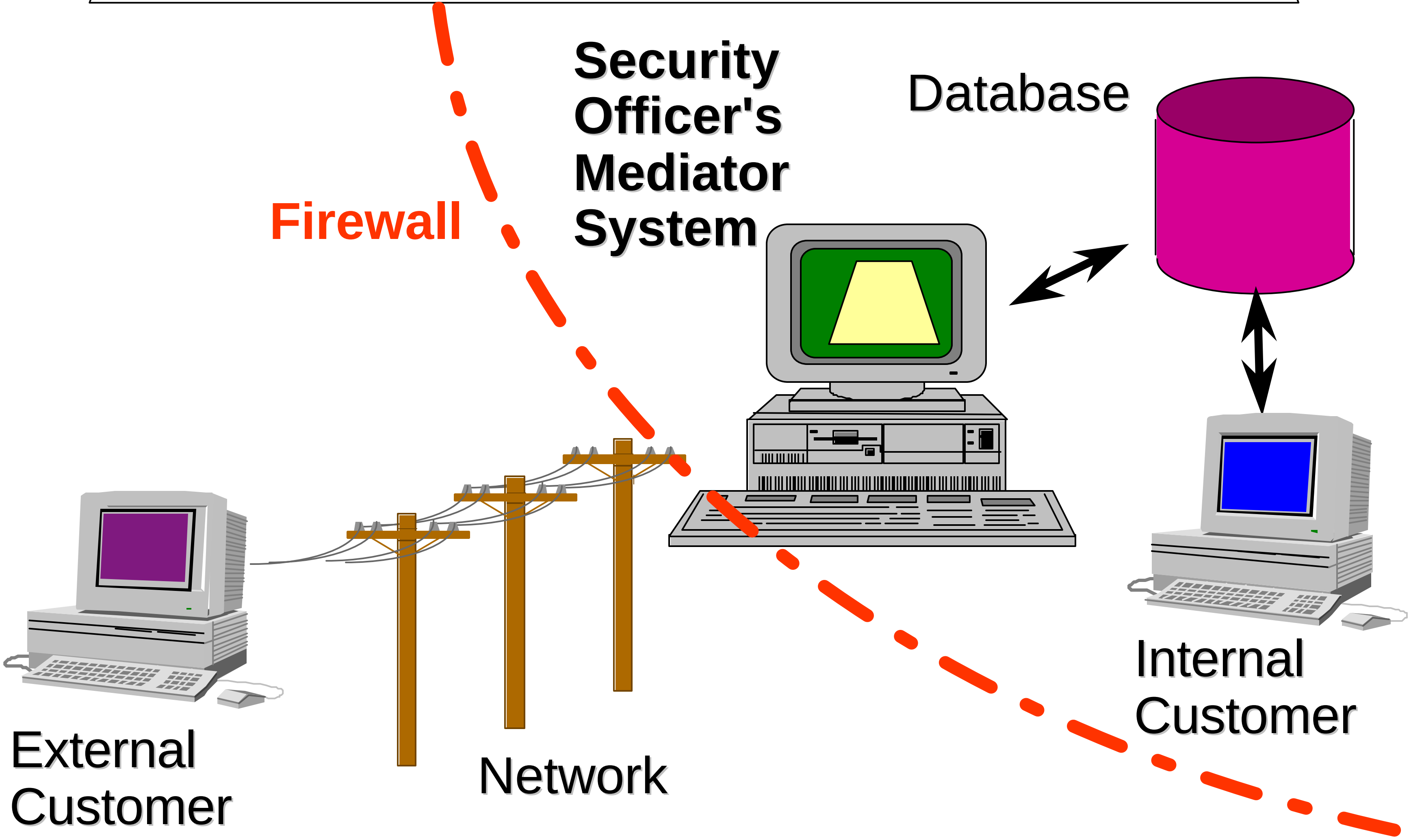
firewall

result

Security mediator : **Human & software agent module**

query

Overall Schematic



Security Officer's Mediator System

Database

Firewall

External Customer

Network

Internal Customer

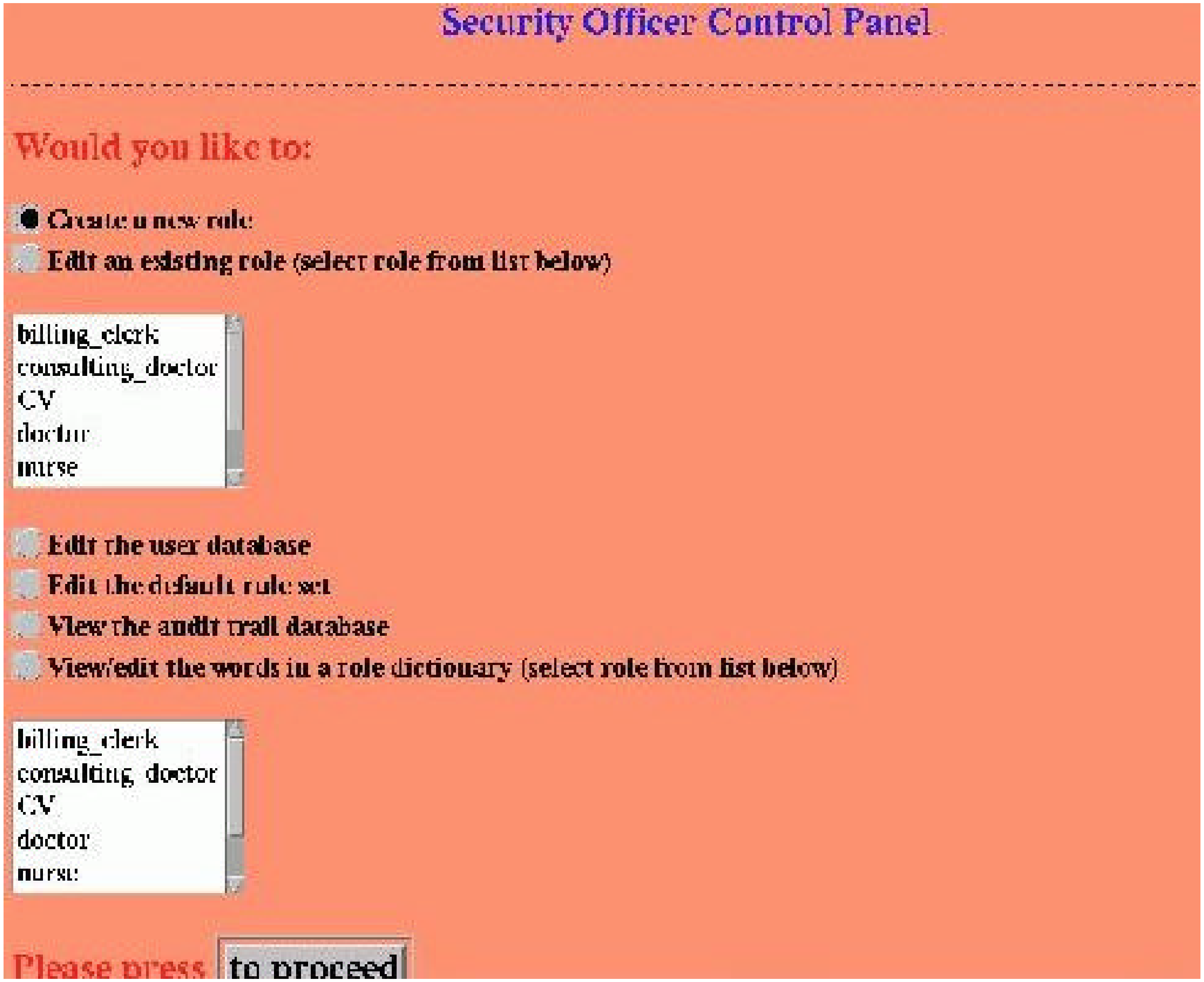
Security Mediator

- System module, intermediate between "customers" and databases within firewall
- Resides on security's officer's machine
  (may have to be multi-level secure);
  accessed via firewall protection by customers
- Under control of security officer,
  via simple security-specific *rules*
- Performs bidirectional screening
  (queries and results)

Security Officer ☹

- **Profile**
  - **Human responsible for database security/privacy policies**
  - **Must balance data availability vs. data security/privacy**
- **Tasks (current)**
  - **Advises staff on how to try to follow policy**
  - **Investigates violations to find & correct staff failures**
  - **Has currently no tools**
- **Tasks (with mediators)**
  - **Defines and enters policy rules in security mediator**
  - **Monitors exceptions, especially violations**
  - **Monitors operation, to obtain feedback for improvements**

Security officer screen



Security Officer Control Panel

Would you like to:

● Create a new role

○ Edit an existing role (select role from list below)

billing_clerk
consulting_doctor
CV
doctor
nurse

○ Edit the user database

○ Edit the default role set

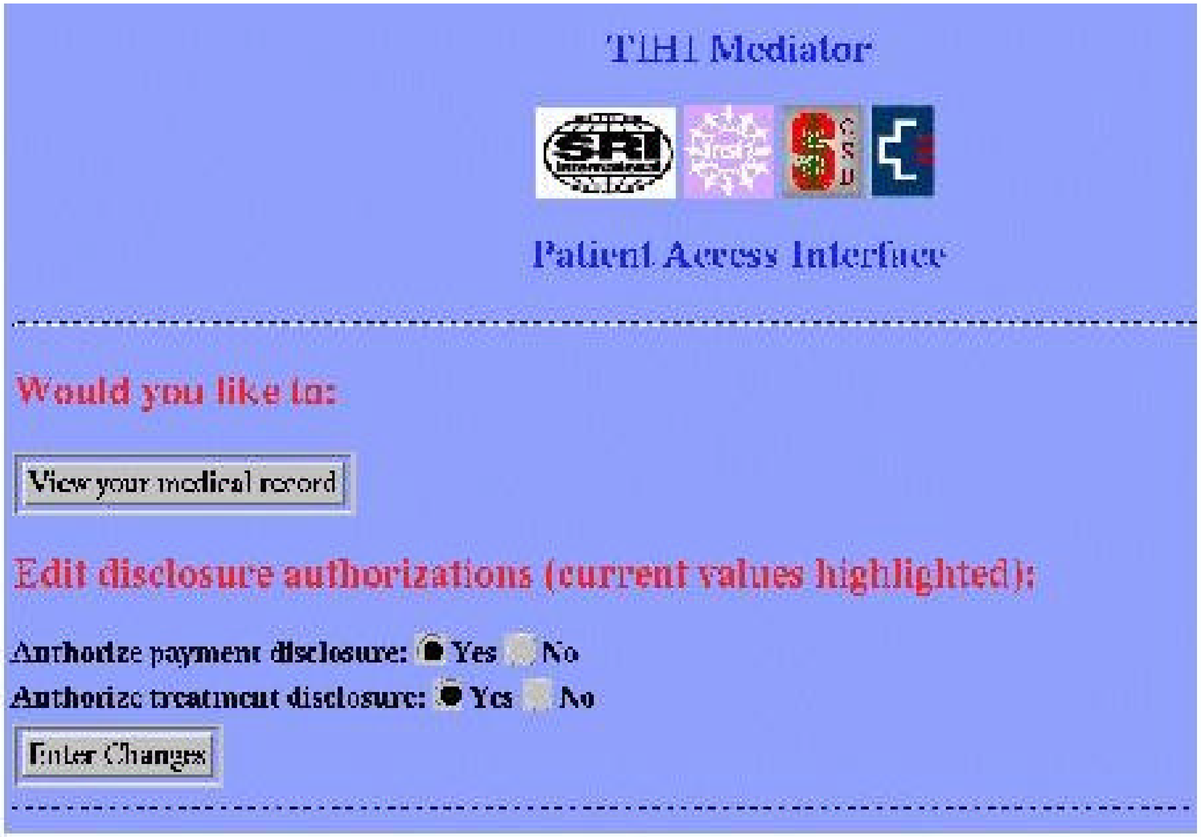
○ View the audit trail database

○ View/edit the words in a role dictionary (select role from list below)

billing_clerk
consulting_doctor
CV
doctor
nurse

Please press

Patient Screen



TIHI Mediator

Patient Access Interface

Would you like to:

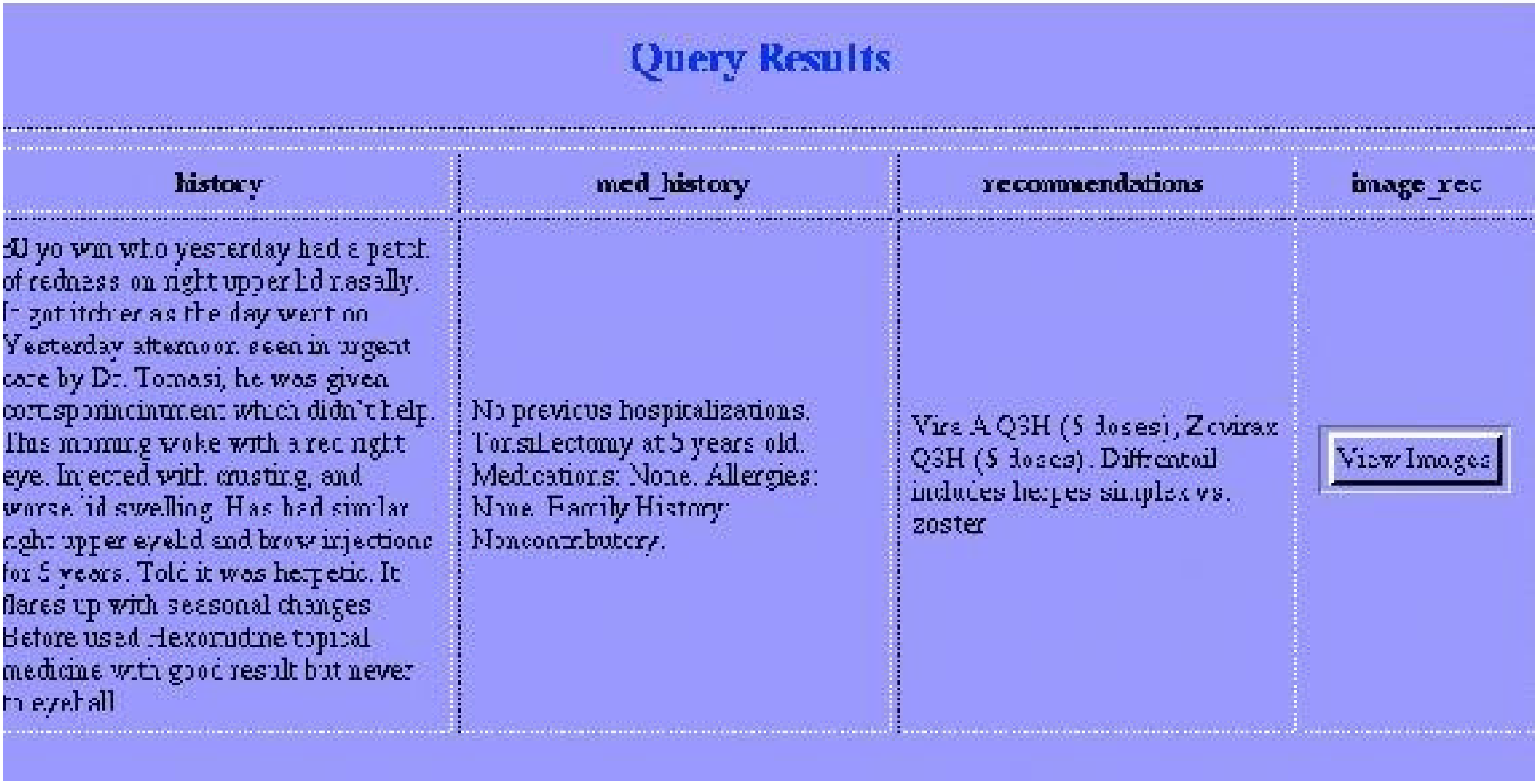
Edit disclosure authorizations (current values highlighted):

Authorize payment disclosure: ● Yes ○ No

Authorize treatment disclosure: ● Yes ○ No

The policy of the institution has been set so that a patient is permitted to see all of his/her own data.

part of Patient result



Query Results

history	med_history	recommendations	image_rec
40 yo wm who yesterday had a patch of redness on right upper lid nasally. It got itchier as the day went on Yesterday afternoon seen in urgent care by Dr. Tomasi, he was given cortisporin ointment which didn't help. This morning woke with a red right eye. Injected with crusting, and worse lid swelling. Has had similar right upper eyelid and brow injections for 5 years. Told it was herpetic. It flares up with seasonal changes Before used Idoxuridine topical medicine with good result but never in eyeball	No previous hospitalizations. Tonsilectomy at 5 years old. Medications: None. Allergies: None. Family History: Noncontributory.	Vira A Q3H (5 doses), Zovirax Q3H (5 doses). Differential includes herpes simplex vs. zoster	View Images

Software Components

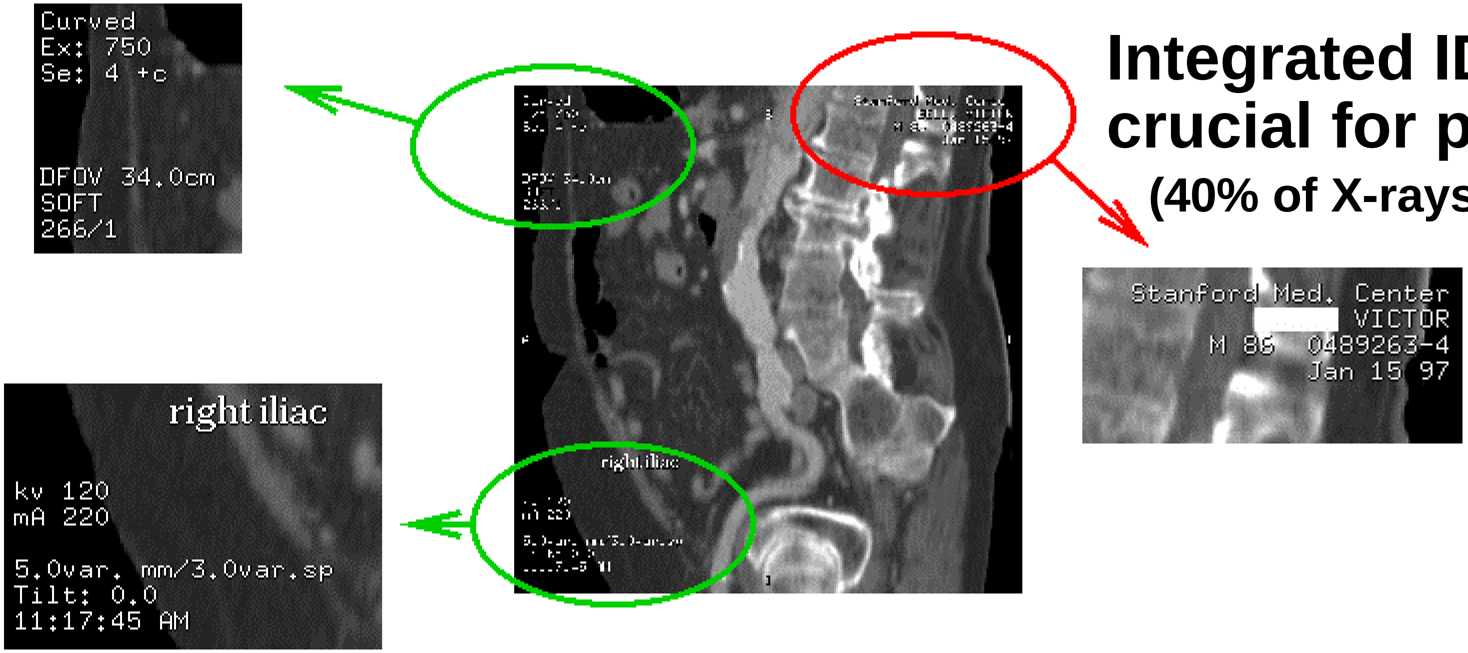
service	• Rule interpreter • Primitives to support rule execution
maintenance	• Rule maintenance tools • Log analysis tool
support	• Firewall interface • Domain database interface • Logger

Primitives

Selected by rule for various clique roles

- Preprocess drawings or **images** to extract information
- Allow / disallow values
- Allow / disallow value ranges
- Limit results to approved vocabulary
- Disallow output containing *bad* words
- Limit output to times, places
- Limit number of queries per period
- etc.

Benign and ID areas in an X-ray



Integrated IDs are crucial for practice

(40% of X-rays are lost)

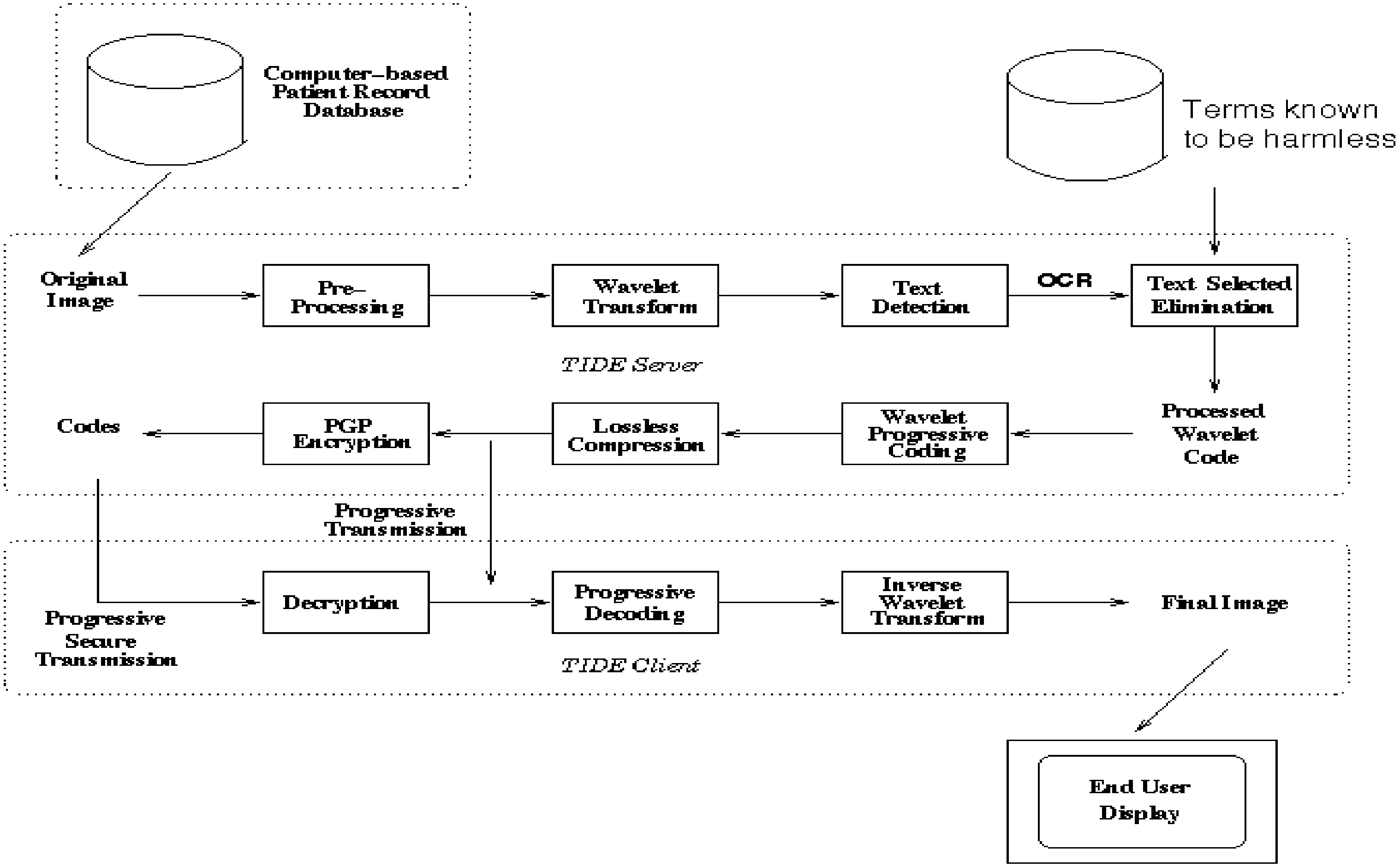
Paranoid: { **Benign is defined positively**

a, value range

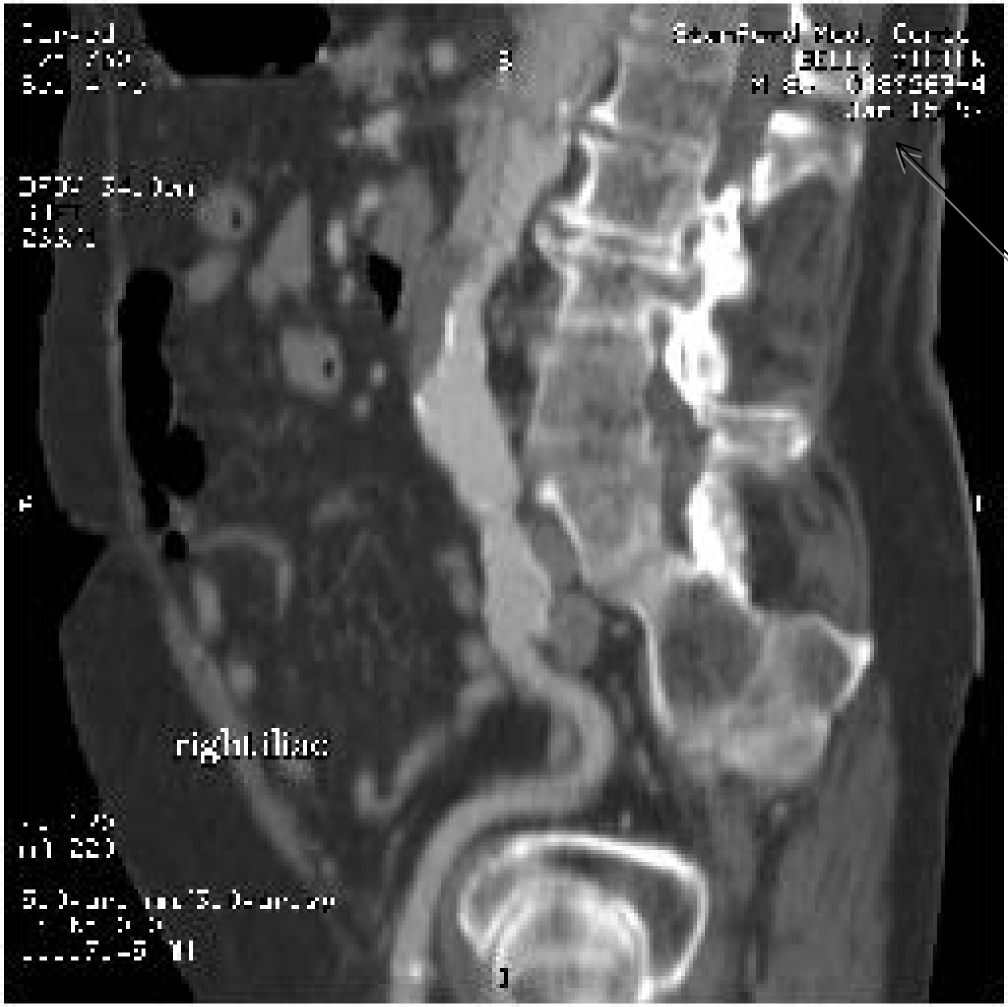
b. good-word list

else it is potentially bad }

Processing Flow

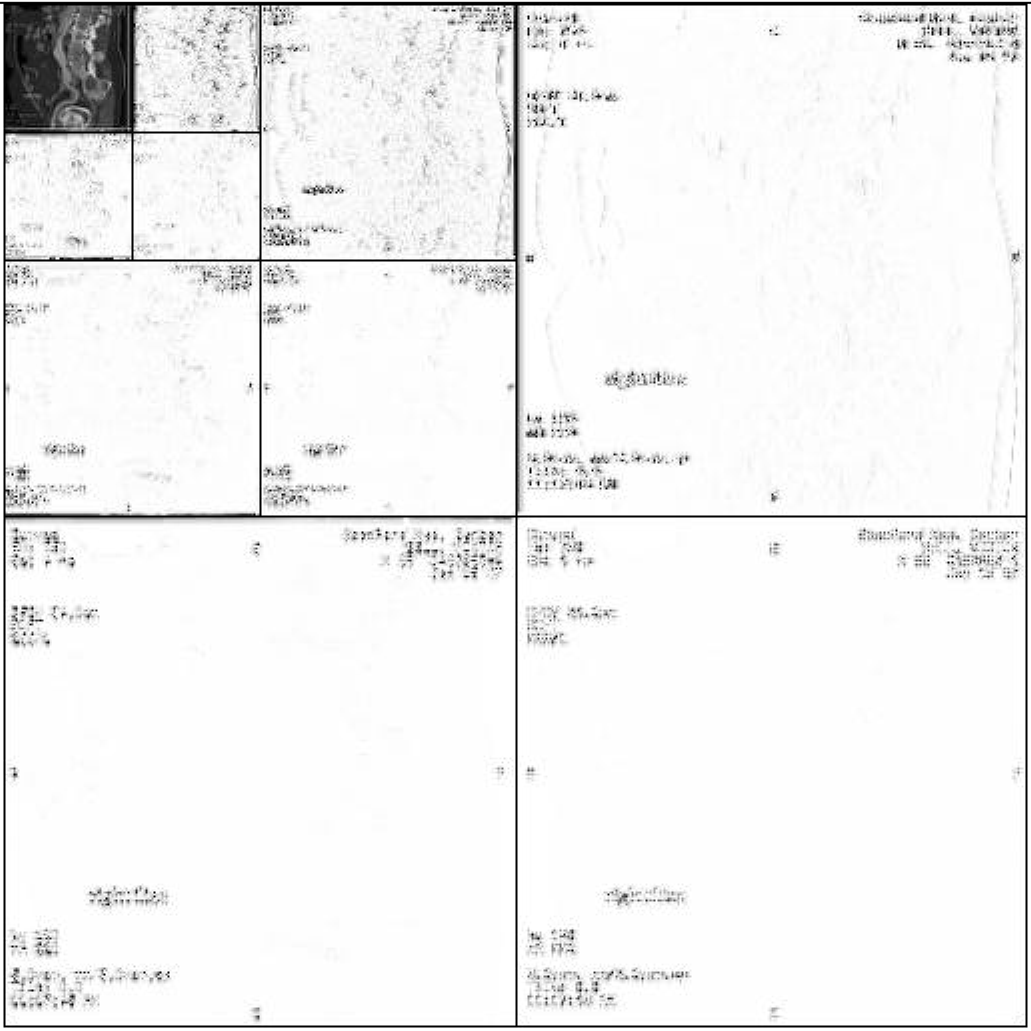


Source X-ray image

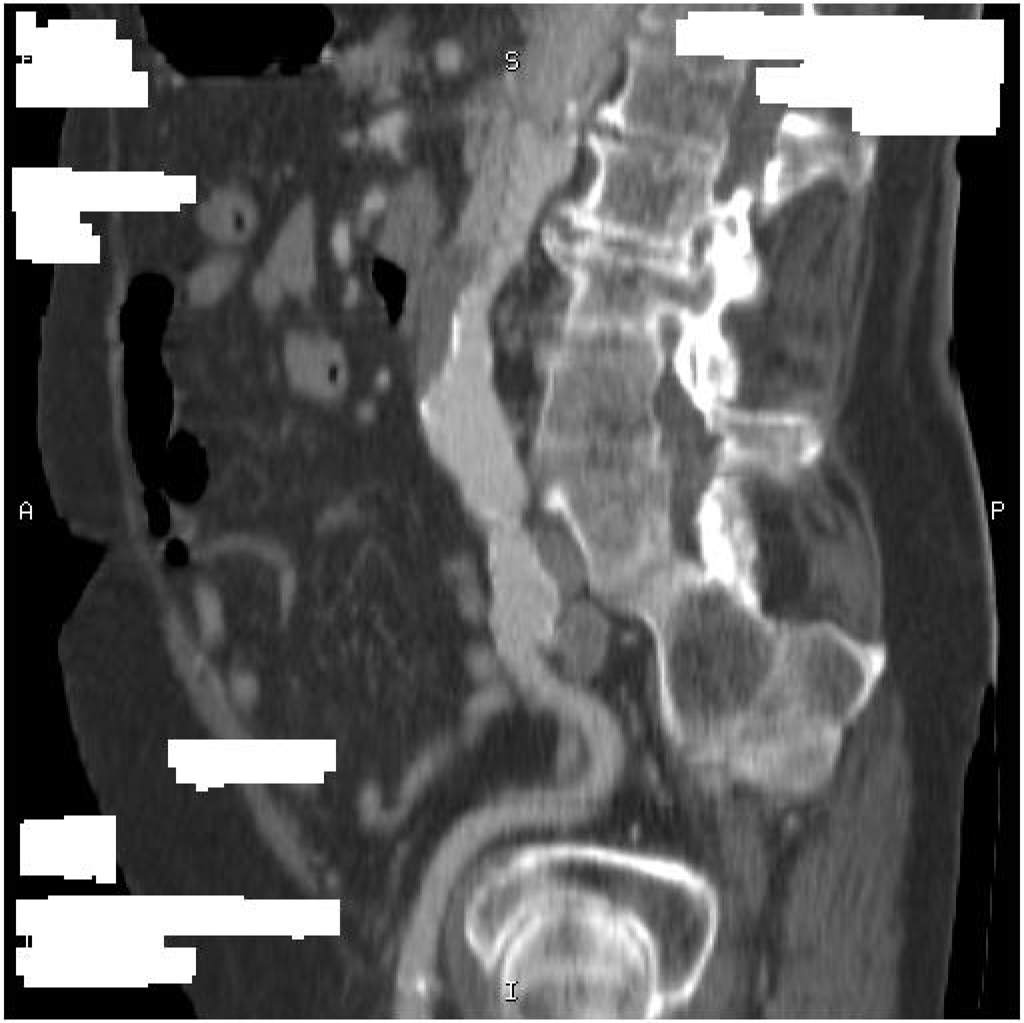


Whitened to protect privacy for this presentation

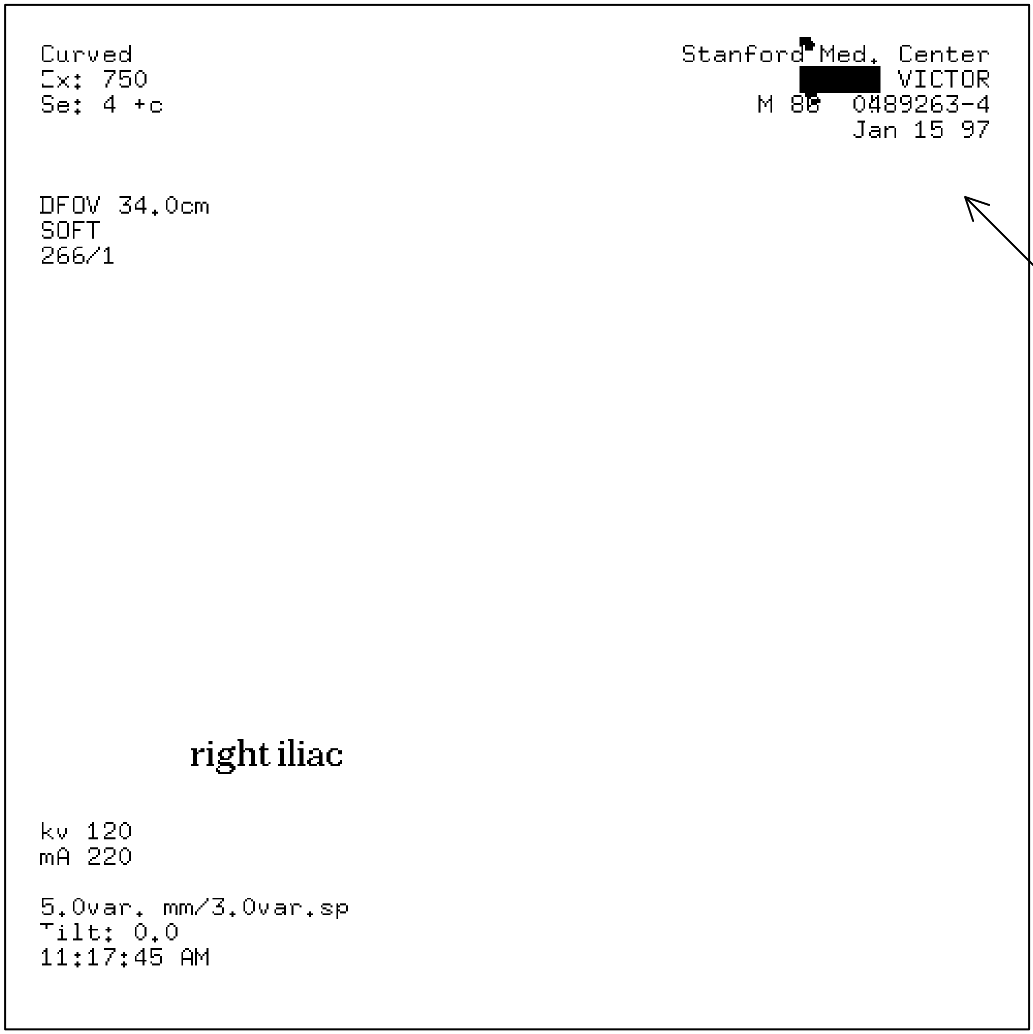
Wavelet decomposition



Candidate Text areas



Extracted textual fields



Curved
Ex: 750
Se: 4 +c

Stanford Med. Center
[redacted] VICTOR
M 86 0489263-4
Jan 15 97

DFOV 34.0cm
SOFT
266/1

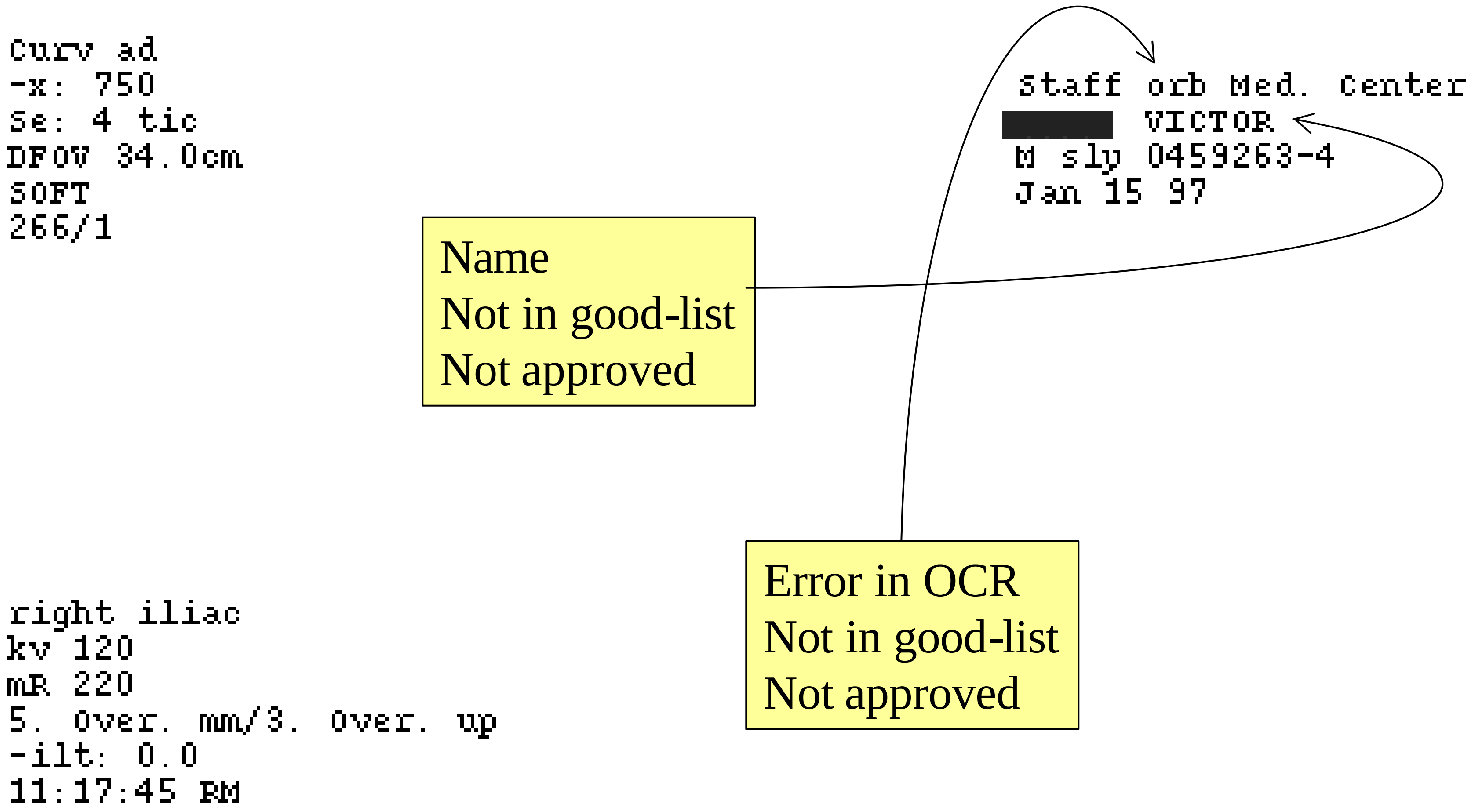
right iliac

kv 120
mA 220

5.0var. mm/3.0var.sp
Tilt: 0.0
11:17:45 AM

Blackened to protect privacy for this presentation

OCR conversion & analysis



```
Curv ad
-x: 750
Se: 4 tic
DFOV 34.0cm
SOFT
266/1
```

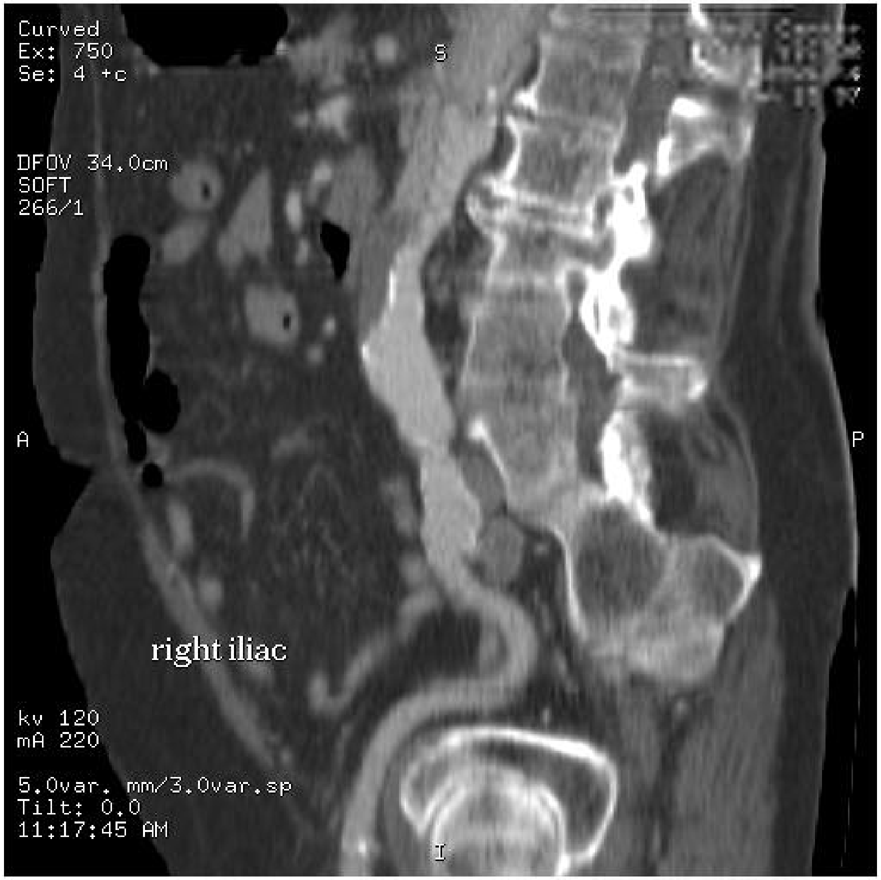
```
Staff orb Med. Center
[redacted] VICTOR
M sly 0459263-4
Jan 15 97
```

Name
Not in good-list
Not approved

Error in OCR
Not in good-list
Not approved

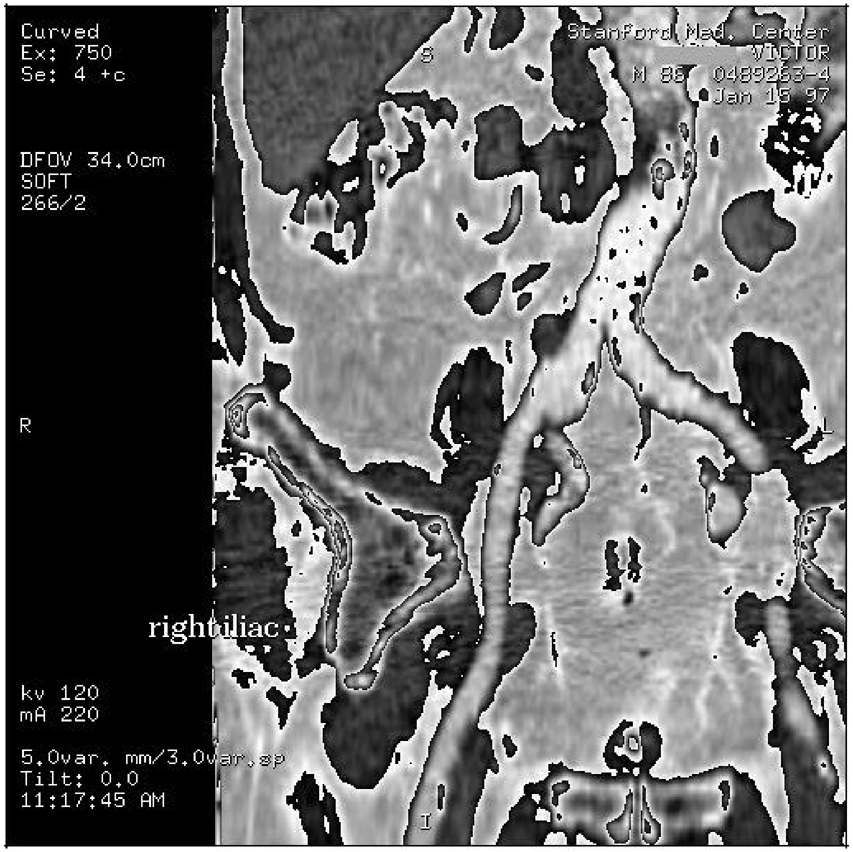
```
right iliac
kv 120
mR 220
5. Over. mm/3. Over. up
-ilt: 0.0
11:17:45 RM
```

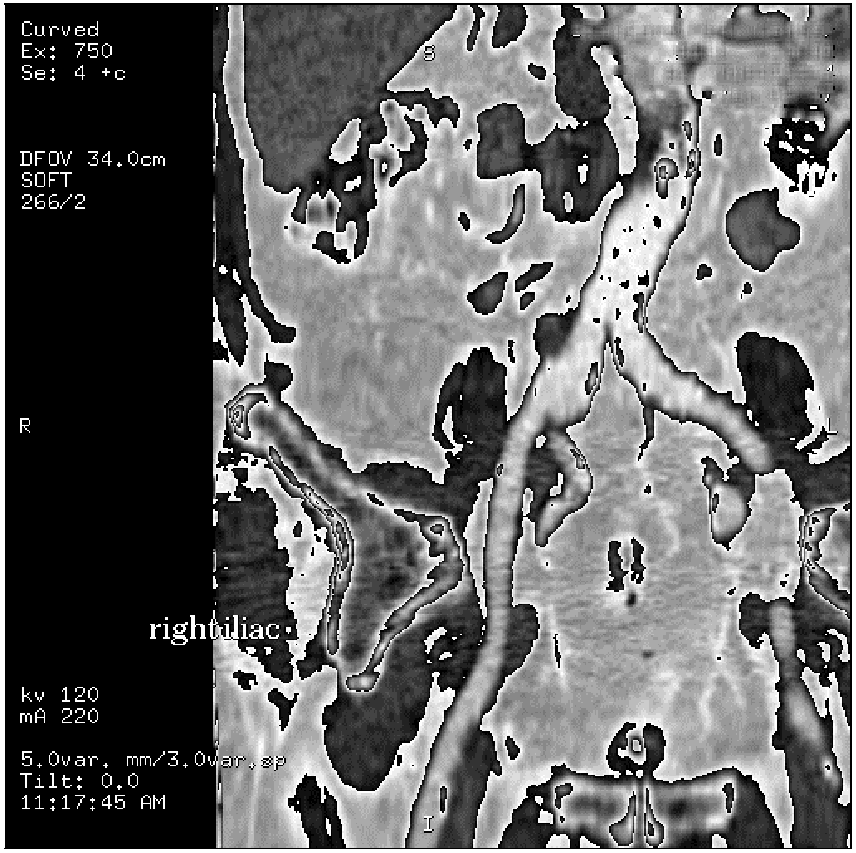
Reconstituted image



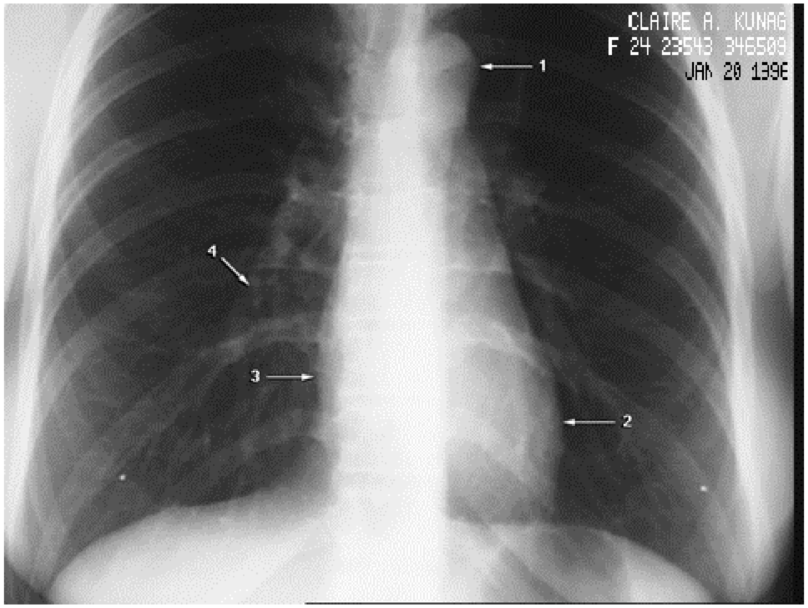
Identification area blurred by removing high frequency components

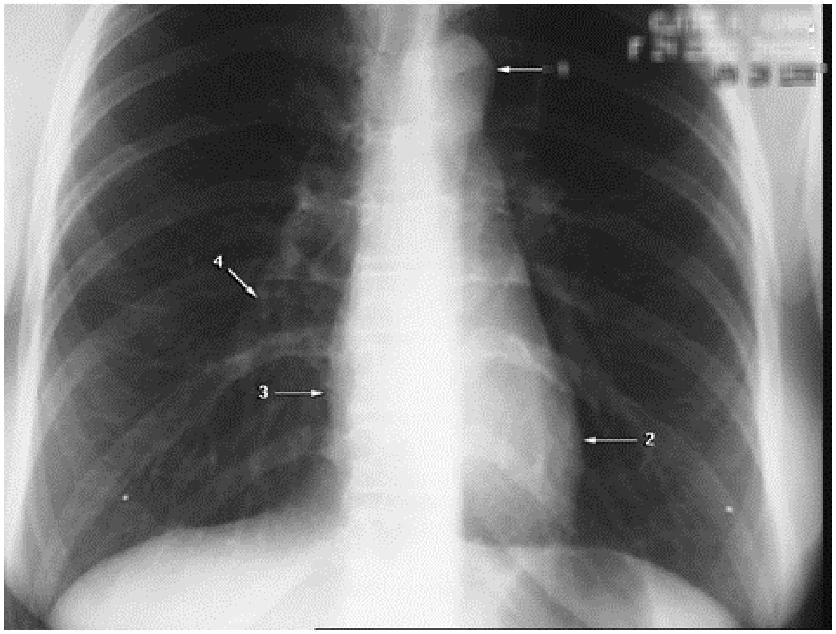
Removal of Ident's from an MRI Image

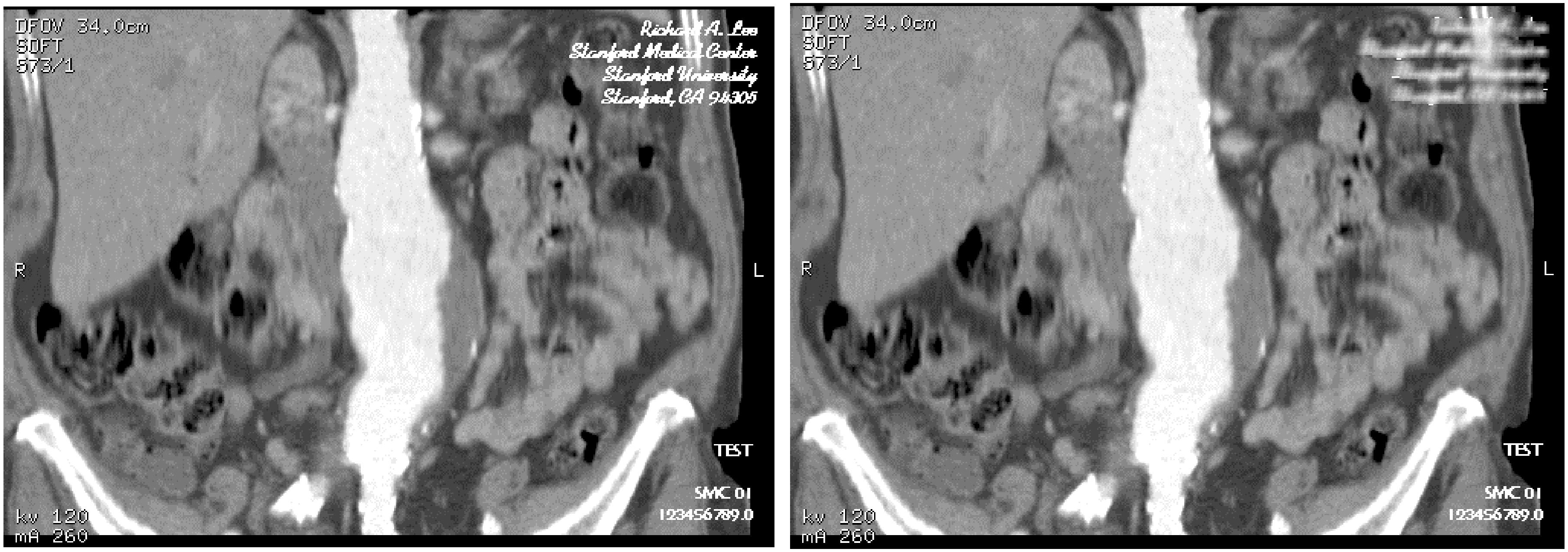




Chest X-ray






DFOV 34.0cm
SOFT
573/1
Richard A. Lee
Stanford Medical Center
Stanford University
Stanford, CA 94305
R
L
TEST
SMC 01
123456789.0
kv 120
mA 260
DFOV 34.0cm
SOFT
573/1
R
L
TEST
SMC 01
123456789.0
kv 120
mA 260

Rule system

- **Optional: without rules every interaction goes to the security officer (in & out)**
- **Creates efficiency: routine requests will be covered by rules: 80% instances / 20% types**
- **Assures Security officer of control: rules can be incrementally added / deleted / analyzed**
- **Primitives simplify rule specification: source, transmit date/time, prior request, ...**

Primitives get data for Rules

- **Requestor roles**
- **Data names requested and values returned**
  - **dates**
  - **value ranges**
  - **textual contents --- positive / negative**
  - **special indicators: employment, …** ***[Scrub ..]***
- **Size of base leading to a statistical result**
- **Time and place of request & destination**
- **Interaction history: frequency, overlaps, . . .**
- **Measure of Risk:** ***[Datafly]***
- ***more . . . .***

Participants in Setting Rules

Security officer manages security policy,

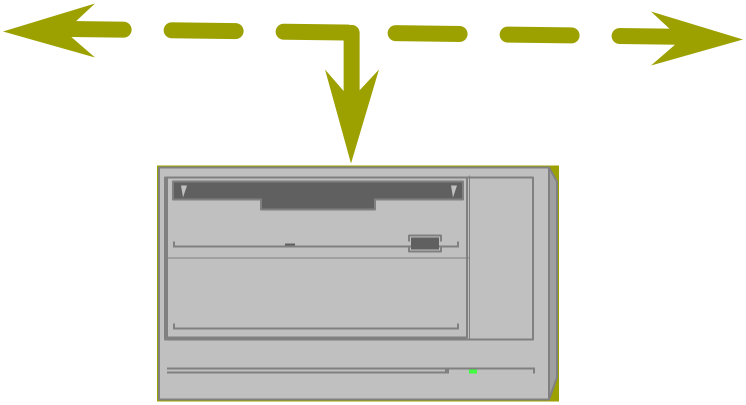
not a computer specialist or database administrator.

Computer specialist provides tools

agent workstation program for security mediation

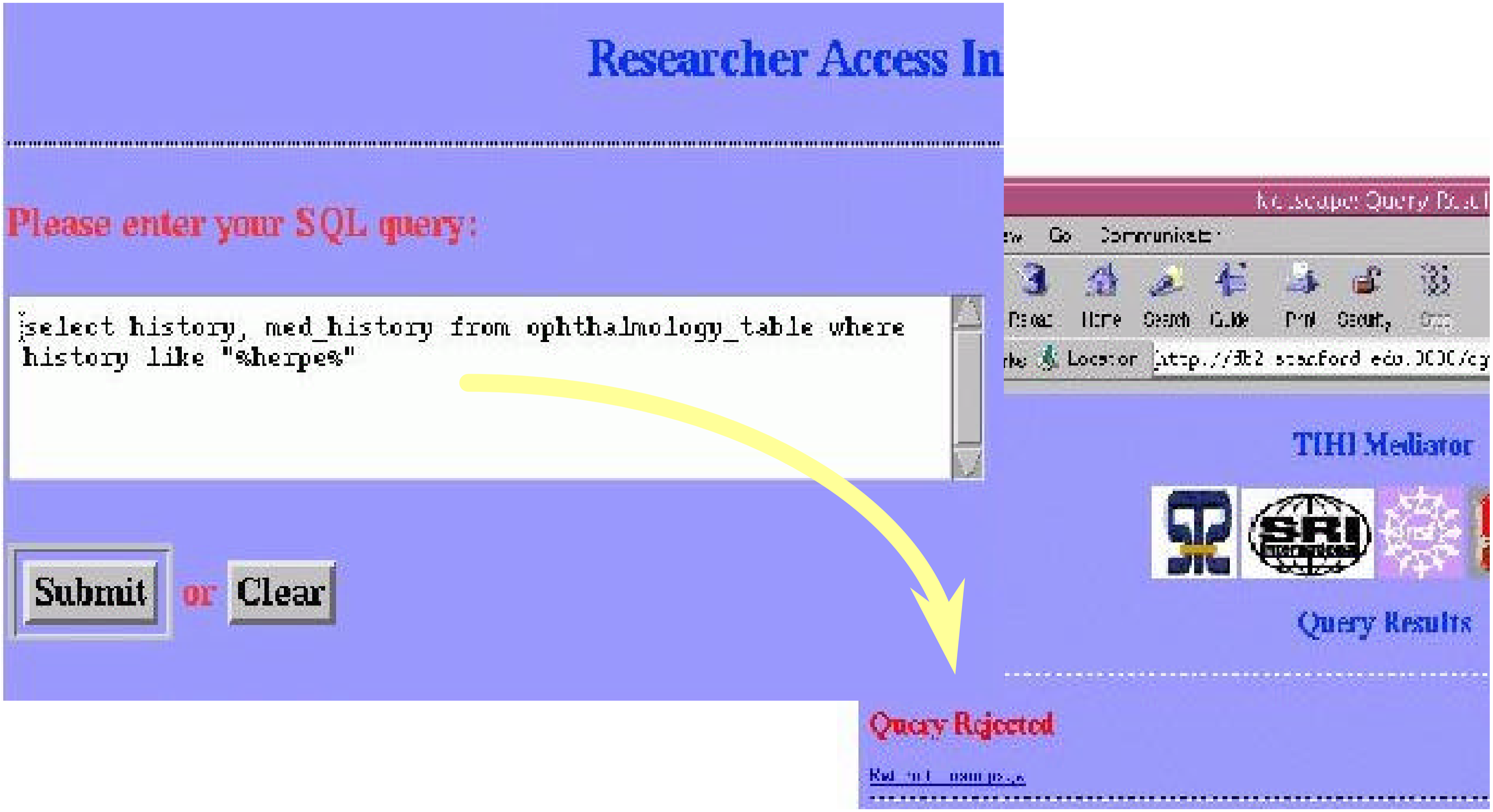
Healthcare institution defines policies

its security officer uses the program as the tool



- **Tool provides logging for**
  - **system improvements**
  - **audit trail**
  - **accountability**
- **Formalizes *ad-hoc* practices**

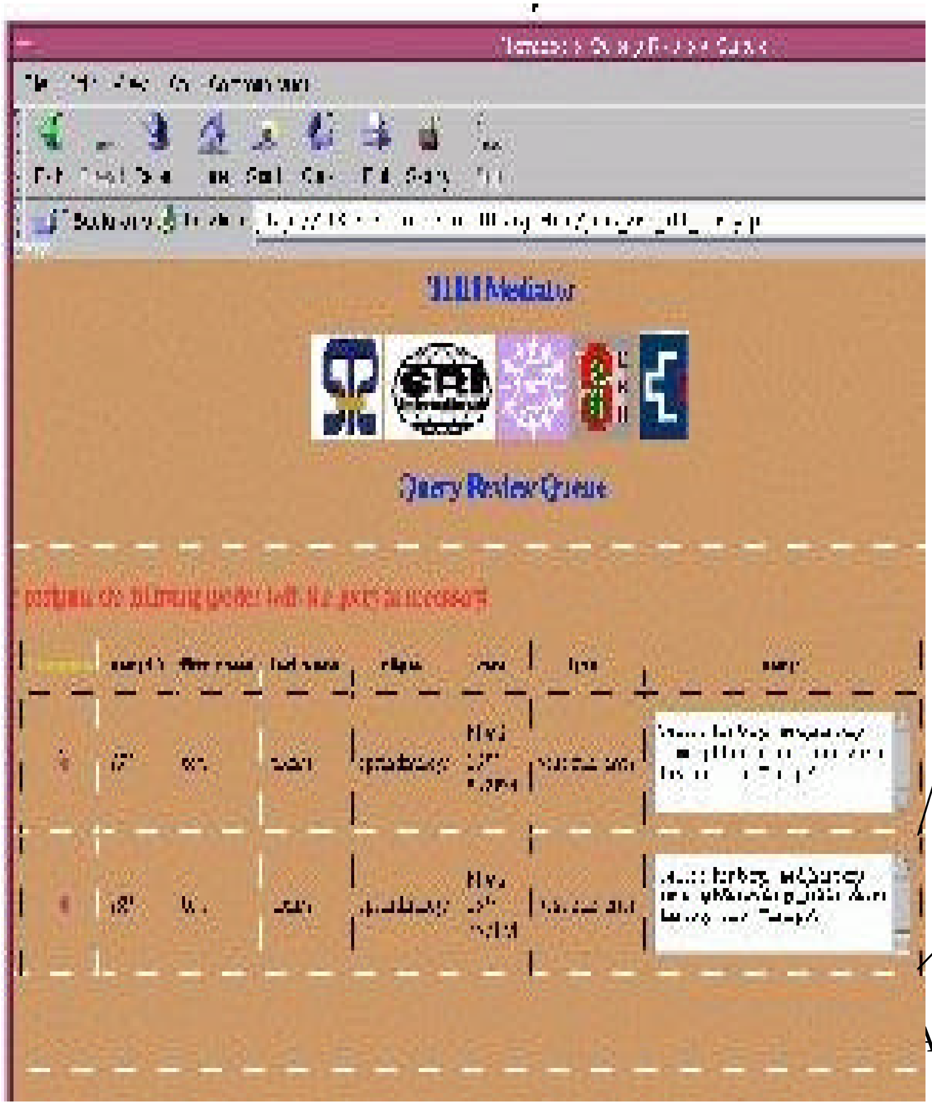
Disallowed result

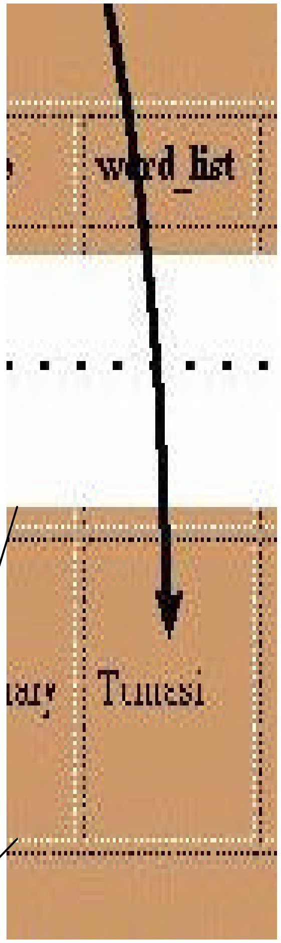


```
select history, med_history from ophthalmology_table where
history like "%herpe%"
```

Query Rejected

Security officer reaction



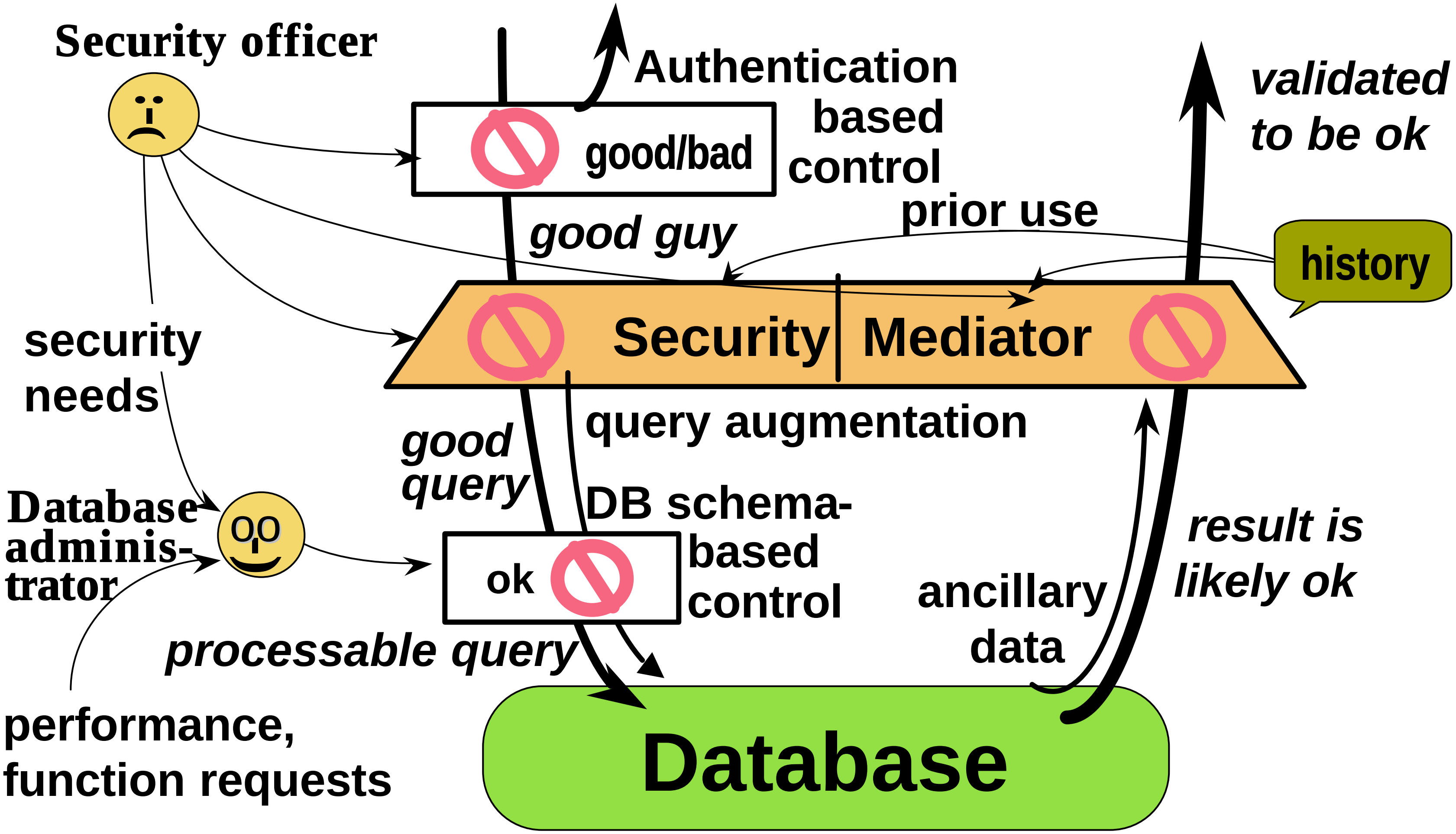


Choices:

1. Reject result
2. Edit result
3. Pass result

(& Update the list of good-words, making approval persistent)

Coverage of Access Paths



Security Mediator Benefits

- Dedicated to security task (may be multi-level secure)
- Uses only its rules and relevant function, all directly, avoids interaction with DB views and procedures
- Primitives simplify rules - can drive image processing
- Maintained by responsible authority: the security officer
- Policy setting independent of database(s) and DBA(s)
- Logs just those transactions that penetrate the firewall, records attempted violations independent of DB logs*
- Systems behind firewall need not be multi-level secure
- Databases behind firewall need not be perfect

* also used for replication, recovery, warehousing