

Dataprotection in Hospitals

Bart Van den Bosch

CIO UZ Leuven

March 4, 2008

- Situation of hospital data protection
- (Physical security)
- System data protection
 - Availability & Integrity
 - Confidentiality
- Network security
- Application level data protection

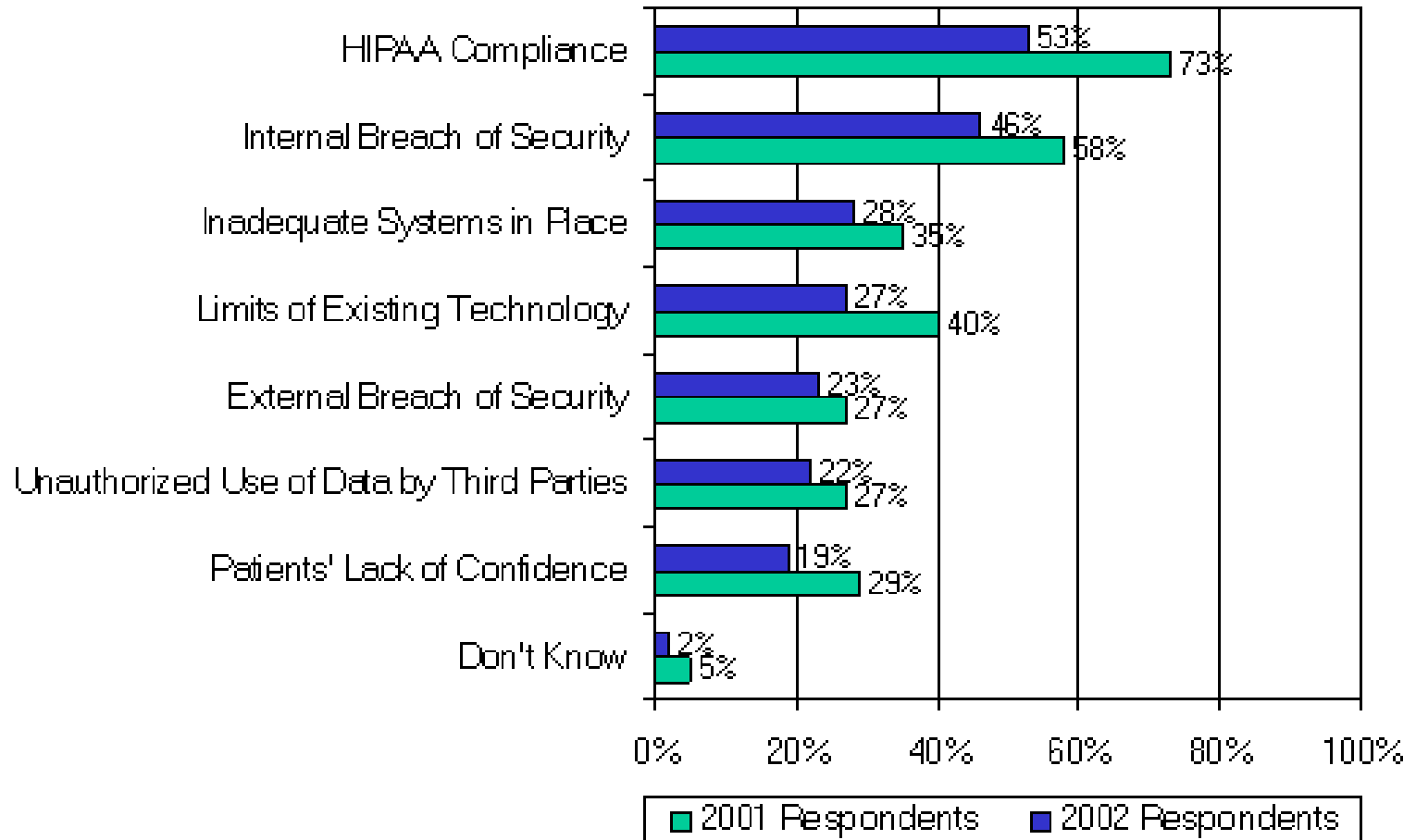
- Enemy is difficult to define
- Everybody is a VIP to somebody
- Curiosity is the driving factor
 - Everyone is curious to some degree
 - Impossible to screen personnel on curiosity

**You can at best control legitimate access,
You can never control legitimate use.**

Threats

13th Annual HIMSS Leadership Survey 2002

Top concerns security electronic patient records:



External Threat

“Two years ago *Sunday Times* reporters were able to gain access to the private medical records of Dr Sandy Macara by paying a small fee to a commercial agency.”

BMJ 1999;318:1328–31

Physical situation

- Open house: lots of strangers near screens
- No physical separation between patients, personnel, visitors, students or external personnel
- No problem if you carry a suitcase (or two)
- Very complex and constantly shifting access needed
 - Depends on workflow: referrals, (abnormal) results, requests,...
- Nurses have short but frequent bouts of workstation work
- Several users simultaneously on same workstation; one user will switch constantly between different workstations.

Requirements on availability

- Nuclear plant
 - Can not afford to go down
 - During maintenance of plant the hardware and software can also be maintained (days, weeks)
 - Historical data is “historical”
- Hospital
 - 5’ down is not too bad, but hours downtime not allowed.
 - No maintenance window whatsoever (migration!)
 - Historical data becomes acute data when patient is in
 - Data loss not allowed (at least not the first 30 years after the death of the patient)

➔ Different system contingency plans!

System data protection: availability

- All storage consolidated on NetApp
- RAID disks with double parity
 - Hot swappable, automatic replacement ordering
- Separate storage clusters for both data and logs (data x 2)
- Problem with clusters
 - Both halves need the same software
 - Corruption in software affects both copies
 - Upgrading the cluster requires taking it down
- Still not possible to upgrade DB software without downtime

Amateurs talk strategy,
professionals talk logistics.

- General Norman Schwartzkopf



Amateurs talk development,
professionals talk migration.

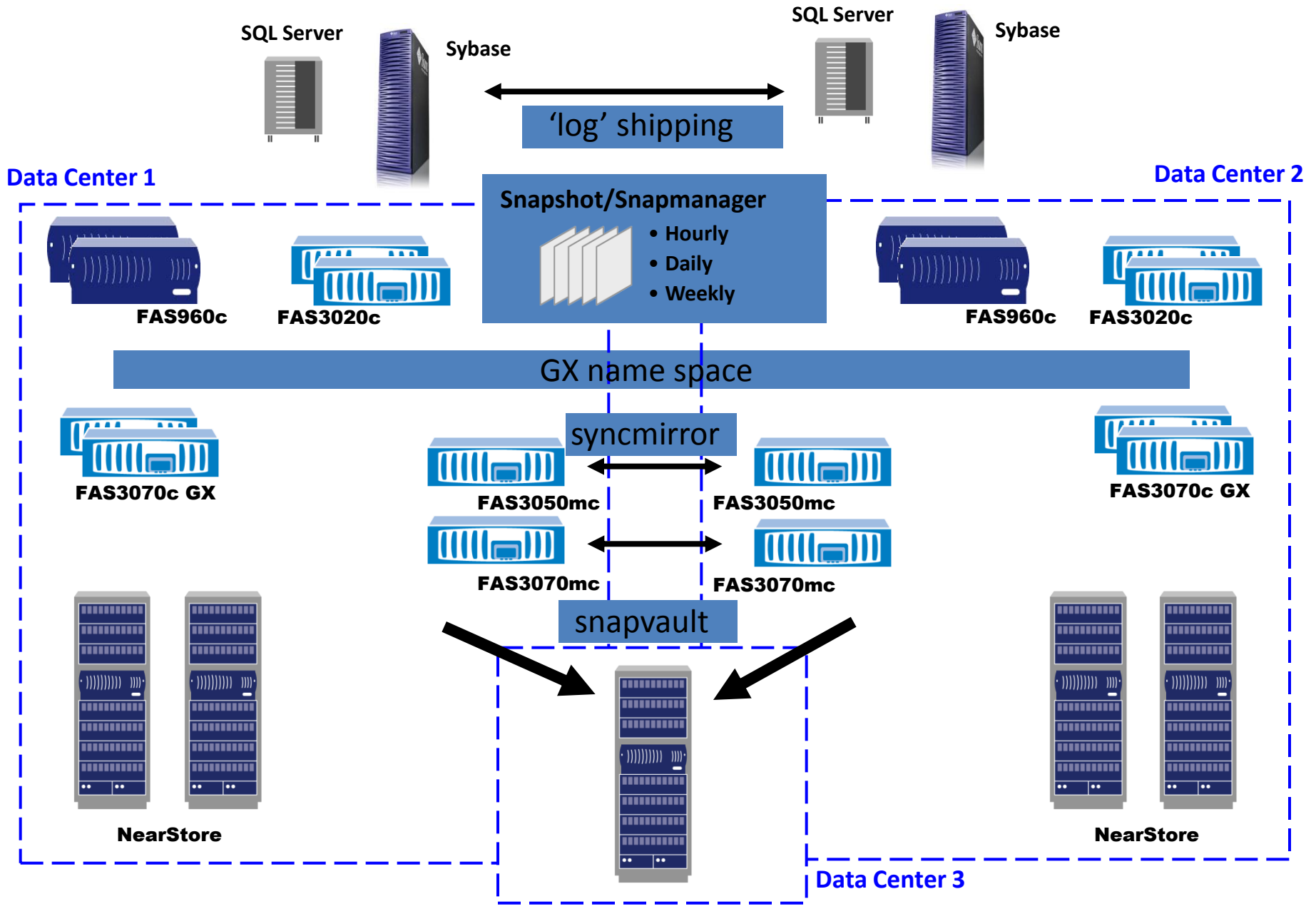
- Prosenior Bart Van den Bosch



Hence:

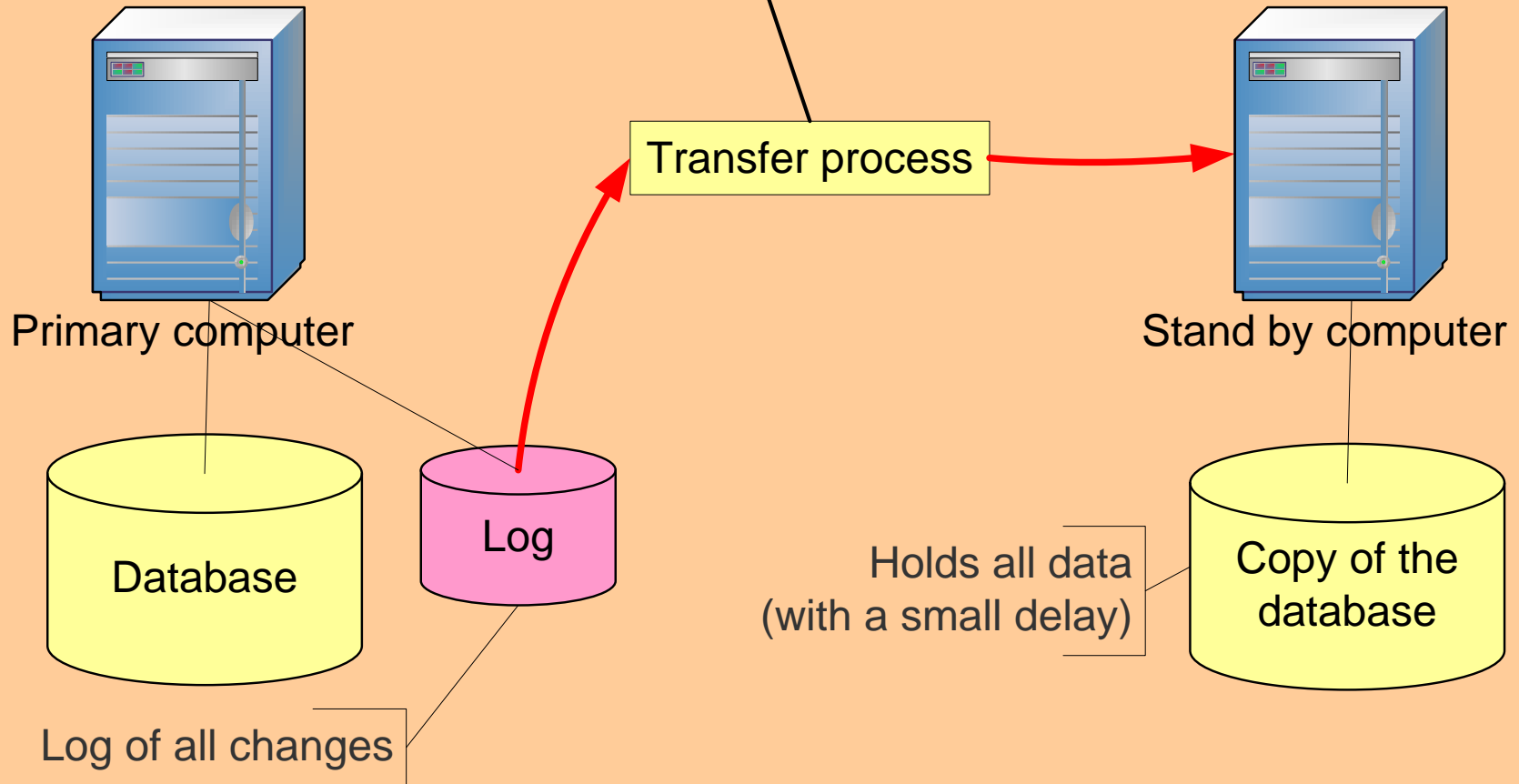
- Identical configuration in 2d data center: hot standby (data x 4)
 - Production can switch from one data center to the other
- Between data centers: logical data replication (sort of log shipping)
 - Data manipulation reduced to very simple insert, update and delete statements
 - Allows to have different versions of database software in both data centers containing same data!

UZ Leuven 500TB NetApp Storage



Replication of a database

Reads all changes and sends them in the form of SQL commands to the stand by server



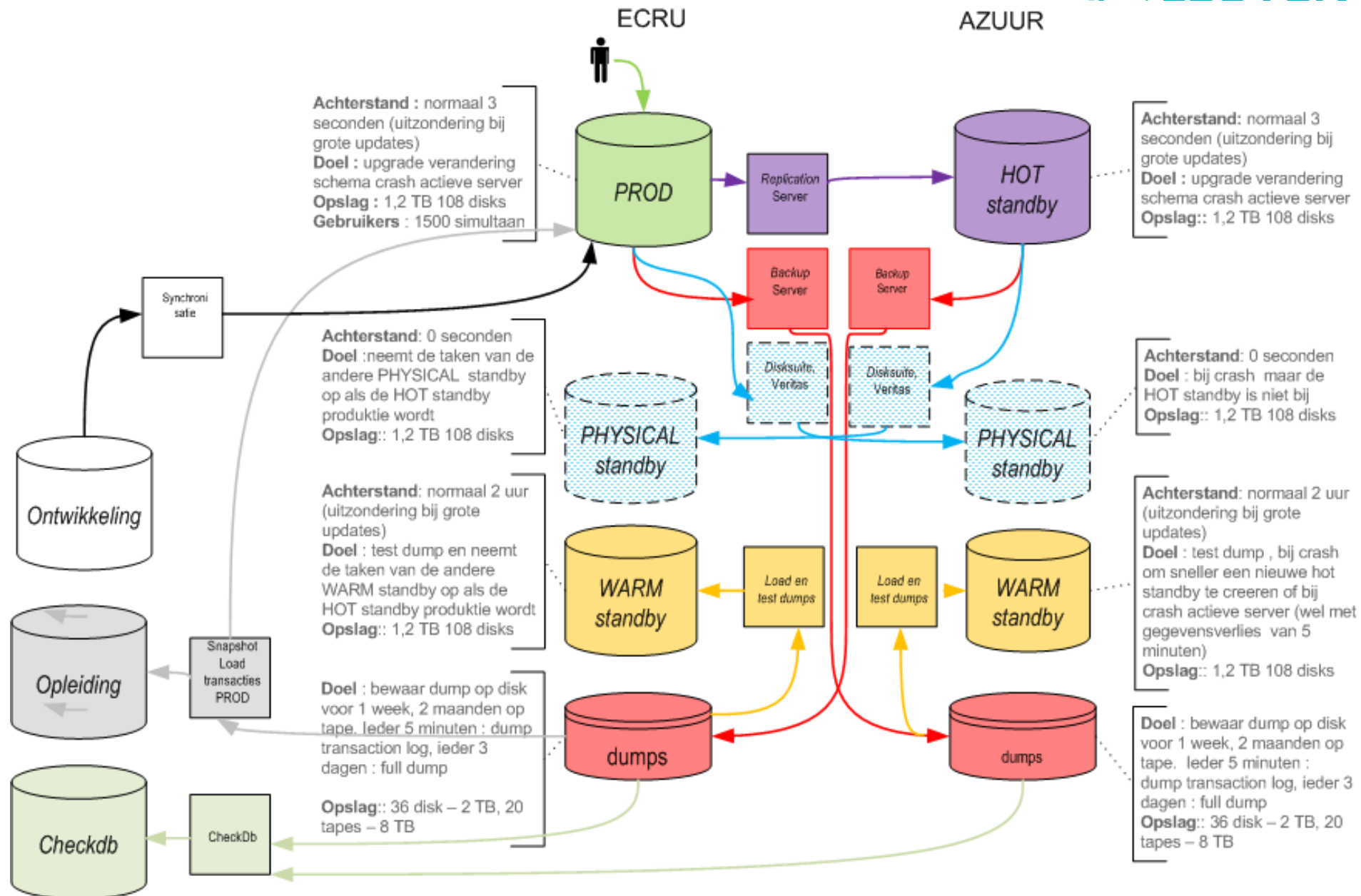
Replication of a database (2)

- Advantage
 - Both servers can run different version of the software
 - ➔ reduces unplanned downtime
- Disadvantage
 - Not a simple set up!
 - Standby computer is a passive computer: expensive!
 - Can be used for a limited number of tasks

But...

- Still problems with application bugs that corrupt data
- Programmers going ape...
- Hence: **warm standby** (data x 5)
 - Smaller configuration
 - Loaded with backup of production data
 - Gets all logs applied but with a time delay of $\pm 6h$
- Gives us 6h to detect corruptions
- BONUS: Continuous sanity check of backups & logs
- (BTW: Backup on disk → fast restore (data x 6))

Clinical data protection



Authentication (within hospital)

- (Still) username & password
 - Passwords only 3 months valid
 - Can not be repeated
 - Must be 8 chars long & 2 char sets
 - Parts of 4 chars and more should not be known words
- Why? Ergonomics! All other solutions either insecure or slow...
 - Maybe fingerprint recognition in future?
 - 14.000 fingerprints is BIG for any current system

- The usual stuff: database authorisation matrix
 - Expressivity is too low for fine grained access control → done on appl level (see later)
- System logs:
 - We do not have/cannot afford/do not want separate deployment and development teams
 - Programmer actions are logged on system level
 - 4 eyes principle (but within department)

Password policy

- Single sign on: we do not allow separate logins for different applications → if your password is known, others have access to
 - your email, your personal files, your credit accounts, your vacation chart, and (soon) your salary
- Everybody gets a login. There is never a reason to use somebody else's.

Authentication from outside

- Juniper for encryption
- Digipass from Vasco
 - Radius server
- Requires all users to be known and registered
- For patient access: Belgian eID card or “token”



Application level

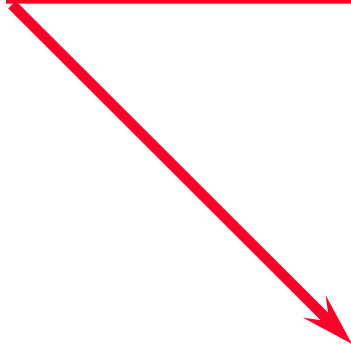
- Authentication
- Access control
- Logging and audit
- Procedures
- Emergency procedures

- ERGONOMICS!!!
- Switch users without stopping application
- Screenblanker after 12 min
 - Same user returns → same windows
 - Other user → most windows close but some censuslists, worklist remain open
- 12 min ← long enough to allow physician to do part of examination
 - In operating room: no screenblanker

Dynamic Access Control

	Report	Validation	Activities	Appointments
Physician	●		●	●
Supervisor	●	●	●	●
Nursing			●	●
Administrative	●			●
...				

Patients



(In many systems this axis is not used)

User must have access to info on a patient “when there is a medical need-to-know”.

- = if user is involved in treatment
- = if contact between user and patient OR
- = if appointment planned OR
- = if examination request for that user OR...

- “Need to know” is not an algorithm
- Is data available to deduce the need to know?
 - Full integration of all systems necessary
 - ➔ Full integration of management necessary
 - Deduction only from data already registered, not on intention!
- Emergency access should always be possible

Deducing “the need to know”:

- Location of patient
 - Every physician, nurse,... is associated with a ward and or department
- Is there an active relationship between physician and patient (usually ends with a validated report)
 - Grace period of access after validation
- Appointment planned?
- Operation planned or requested?
- Technical examination planned or requested?
- Request to other physician to look into the case?
- ...

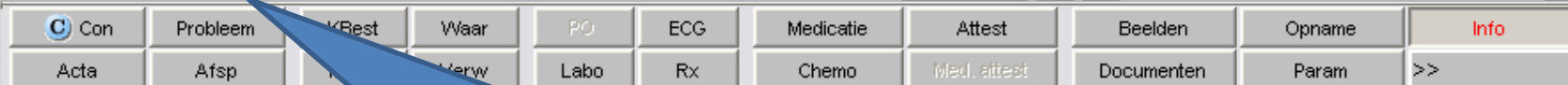
LISA: other access model

- LISA = Leuvense Internet Samenwerking Artsen
- Referring physicians access the medical file within UZ for their patients
 - Access to complete file, not only reports addressed to them
 - Allows them to give better service to patients and family
- Informed consent necessary: 99.5% of patients signs
 - We do not have the info to deduce “need to know”
 - Less social control
- Currently “opt in”, going to “opt out”
 - Only for General practitioners

- The Clinical Workstation data model is deletionless
 - Update = logical delete old record + insert corrected record + link between these
 - Delete = logical delete
 - Everything = timestamped + username recorded
- Enforced on database level
- State of data base can be reconstructed to any point in time

Logs: user level

- Access given ONLY AFTER “need to know” for specific patient and user combination is checked
- If OK → normal access, no logging
- If NOT OK → user has to overrule
 - Reason needs to be given
 - All accesses are logged
 - Treating physicians can see the overrule logs for their patients



Algemene info

Naam: KWS-DEMOPATIENT
Eadnr: 70 **Emdnr:** 771
SisNr: 771118 123 45

Geboortedatum: 18-11-1

Adressen

Thuis-adres: BEVRIJDIN

Tel/gsm

Telefoon: 123456789

Mutualiteit, verzekeringen en andere organismen

Artsen

Huisarts: Dr. Mertens Ferdinand, Steenweg op Nieuwrode 41, 3111 Wezemaal, tel 016/581367

Moeder-kind relaties

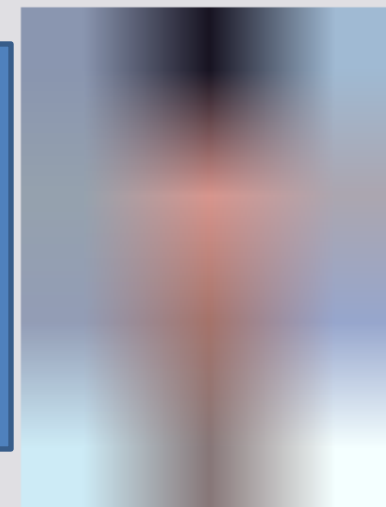
kinderen: DEMOPATIENT KIND (666,000627B218)

Extra dossiernummers

-

File is locked

← system can not deduce
a relationship between
user and patient



Neem foto

Request for overrule reason

Pt. - KWS-DEMOPATIENT NUMMER 70 (70, 771118V999, 30j)

Acties Dossier FONA ▼ REV 0 revalidatie (diffool/ydconi0) ?

Con	Probleem	KBest	Waar	PO	ECG	Medicatie	Attest	Beelden	Opname	Info
Acta	Afsp	MVer	Verw	Labo	Rx	Chemo	Med. attest	Documenten	Param	>>

[Algemene info](#)
Naam: KWS-DEMOPATIENT NUMMER 70
Eadnr: 70 **Emdnr:** 771118V999 **Geslacht:** vrouw
SisNr: 771118 123 45
Geboortedatum: 18-11-1968

[Adressen](#)
Thuis-adres: BEVRIJDIJ

[Tel/gsm](#)
Telefoon: 123456789

[Mutualiteit, verzekering](#)
-

[Artsen](#)
Huisarts: Dr. Mertens Fe

[Moeder-kind relaties](#)
kinderen: DEMOPATIEN

[Extra dossiernummers](#)
-

Overrule

DOORBREKING VAN DE TOEGANGSBEPERKING!

U heeft geen toegang. Geef een geldige reden indien u toch toegang wenst.
WAARSCHUWING! Het is een ernstige overtreding indien u zonder geldige reden gegevens bekijkt van een andere dienst!
Als u kan volstaan met de gegevens van deze dienst, gelieve dan hier NIET verder te gaan!
De reden die u hier geeft zal worden nagegaan!

☐ Kankerregistratie
☐ Andere reden:

Annuleer

“You do not have access. Please supply a valid reason. Warning: It is a serious misdemeanour to access data without a valid reason. The reason you supply will be checked.”

Pl. - JANSSEN EDDY (70001219, 520507M029, 55j)

Acties Dossier FONA

Con	Probleem	KBest	Waar	PO	ECG	Medicatie	Attest	Beelden	Opname	Info
Acta	Afsp	MVer	Verw	Labo	Rx	Chemo	Med. attest	Documenten	Param	>>

Algemene info

Naam: J. Janssen
 Eadnr: 70001219 Emdnr: 520507M029 Geslacht: man
 SisNr: 520507M029

Geboortedatum: 1955-08-25 Leeftijd: 55
 Nationaliteit: B
 Verwanten: (echtgenoot) NG K.

Adressen

Thuis-adres: VORVOERSTRAAT 23A, 3320 LONNEL

Tel/gsm

Telefoon: 06-1234567

Mutualiteit, verzekeringen en andere organismen

Mutualiteit: 32200 (DE VOORZORG LIMBURG) Kg1/2: 100000 StamNr: 123456789

Artsen

Huisarts: Dr. M. J. Janssen

Moeder-kind relaties

Extra dossiernummers

Neem foto

Log

- (3) Menten Johan (supervisor), Voorbereiding raadpleging (1)
- (5) Vanderveken Magda (CMA_typpool), brief (1)
- (4) Lenaerts Corinne (administratie), uitslag (1)
- (4) Van Paesschen Raf (assistent), opgebeld door perifere apotheker ivm behandeling (1)
- (2) Beerens Ann (administratie), komt op 27/08 (1)

Automatic popup when opening patient file. Disappears automatically after a few seconds (or by closing it)

Pl. - JANSSEN EDDY (70001219, 520507M029, 55j)

Acties Dossier

Con Probleem KBest Waar PO ECG Medicatie Attest Beelden Opname Info

Acta Afsp MVer Verw Labo Rx Chemo Med. attest Documenten Param >>

Algemene info

Naam: J. Janssen
 Eadnr: 70001219 Emdnr: 520507M029 Geslacht: man
 SisNr: 520507M029

Geboortedatum: 1955-08-29 Leeftijd: 55
 Nationaliteit: B
 Verwanten: (echtgenoot) NG K.

Adressen

Thuis-adres: V. Janssen, 1000 Brussel

Tel/gsm

Telefoon: 0 20 123 45 67

Mutualiteit, verzekeringen en andere organismen

Mutualiteit: 32200 (DE VOORZORG LIMBURG) Kg1/2: 100000 StamNr: 1000000000

Artsen

Huisarts: Dr. M. Janssen, 1000 Brussel, tel 020 123 45 67

Moeder-kind relaties

-

Extra dossiernummers

-

Neem foto

Popup:

- (3) Menten Johan (supervisor), Voorbereiding raadpleging (1)
- (5) Vanderveken Magda (CMA_typool), brief (1)
- (4) Lenaerts Corinne (administratie), uitslag (1)
- (4) Van Paesschen Raf (assistent), opgebeld door perifere apotheker ivm behandeling (1)
- (2) Beerens Ann (administratie), komt op 27/08 (1)

Automatic popup when opening patient file. Disappears automatically after a few seconds (or by closing it)

Pt. - KWS-TESTPATIENT NUMMER 40 (40, 590804M999, 48j)

Acties Dossier FONA ▼ ONC 0 consultatie (difool/difool)

Con	Probleem	KBest	Vaar	PO	ECG	Medicatie	Attest	Beelden	Opname	Info
Acta	Afsp	MVer	Verw	Labo	Rx	Chemo	Med. attest	Documenten	Param	>>

Algemene info

Naam: KWS-TESTPATIENT NUMMER 40
Eadnr: 40 **Emdnr:** 590804M999 **Geslacht:** man
SisNr: -

Geboortedatum: 04-08-1959 **Leeftijd:** 48j
Nationaliteit: BE

Adressen

Thuis-adres: KURINGERSTEENWEG 504, 1111 WOONPLAATS

Tel/gsm

Telefoon: 123456789

Mutualiteit, verzekeringen en andere organismen

-

Artsen

-

Moeder-kind relaties

-

Extra dossiernummers

-

Neem foto

Number of overrules

User's function

For each overrule where a reason was given, the number of times this reason was used.

(22) Coels Maarten (supervisor), ik (2) - testing (1) - sdf (1)
 (78) Dekinder Pieter (supervisor), testdoeleinden (1) - test+ (1) - test (36)

The popup shows an overview of the last 100 overrules grouped by user.

On clicking the popup a list is given with details of the overrules.


 (1) [De Bolle Lucia](#) (supervisor)
 (7) [Misselyn Dominique](#) (supervisor), *studie* (1)
 (2) [Vermeiren Patricia](#) (trial), *trial* (1)
 (2) [Billet Bart](#) (assistent), *Pre-operatief* (1)
 (1) [Geelen Jos](#) (assistent)
 (1) [Theunissen Mimi](#) (verpleging)
 (5) [Verbruggen Frederic](#) (hoofdverpleging), *opname ort e212* (1)

dyn Overzicht van de gelogde toegangen

☒ Toon laatste 100 overrules

Toon alles (19)
 ● Billet Bart (2)
 ● De Bolle Lucia (1)
 ● Geelen Jos (1)
 ● Misselyn Dominique (7)
 ● Theunissen Mimi (1)
 ● Verbruggen Frederic (5)
 ● Vermeiren Patricia (2)





overruled door	loginnaam	groep	applicatie	datum	type
Vermeiren Patricia	x227212	trial	*	28-01-2000 11:02	externSysteem
Vermeiren Patricia	x227212	trial	*	28-01-2000 11:02	overruled
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:24	beweging
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:24	overruled
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:24	overruled
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:24	overruled
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:25	overruled
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:26	overruled
Misselyn Dominique	dmisse0	supervisor	heelkunde	21-07-2000 10:26	overruled
De Bolle Lucia	ldbolle0	supervisor	anesthesiologie	10-11-2000 08:43	logging
Theunissen Mimi	mtheun0	verpleging	inwendige	31-05-2001 14:25	logging
Geelen Jos	jgeele1	assistent	anesthesiologie	20-11-2001 15:49	logging
Billet Bart	bbille0	assistent	anesthesiologie	03-01-2002 17:09	beweging
Billet Bart	bbille0	assistent	anesthesiologie	03-01-2002 17:09	overruled
Verbruggen Frederic	x218589	hoofdverpleging	heelkunde	28-03-2002 09:18	externSysteem
Verbruggen Frederic	x218589	hoofdverpleging	heelkunde	28-03-2002 09:18	overruled
Verbruggen Frederic	x218589	hoofdverpleging	heelkunde	28-03-2002 09:19	overruled
Verbruggen Frederic	x218589	hoofdverpleging	heelkunde	28-03-2002 09:21	overruled
Verbruggen Frederic	x218589	hoofdverpleging	heelkunde	28-03-2002 09:52	overruled

aantal rijen: 19 / selectie: 0

Sluit
 Vernieuw
 Nieuwe lijst
 Druk selectie




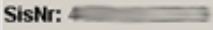
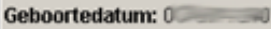

Clicking this button displays the popup again.

Pl. - COX JOZEF (7000-134, 400103M105, 68j)

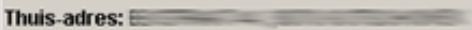
Acties Dossier   **MRSA+** FONA   ▼ GPS 791 gesprek (tdpre1/rvdwyg0) ?

Con	Probleem	KBest	Waar	PO	ECG	Medicatie	Attest	Beelden	Opname	Info
Acta	Afsp	MVer	Verw	Labo	Rx	Chemo	Med. attest	Documenten	Param	>>

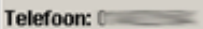
Algemene info

Naam: 
Eadnr:  Emdnr:  Geslacht: man
SisNr: 
Geboortedatum:  Leeftijd: 
Nationaliteit: B


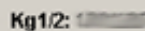

Adressen

Thuis-adres: 


Tel/gsm

Telefoon: 

Mutualiteit, verzekeringen en andere organismen

Mutualiteit:  Kg1/2:  StamNr: 

Artsen


Huisarts: 

Moeder-kind relaties


-

Extra dossiernummers

-



Neem foto

 (23) Delvaux Katrien (assistent), consult (1)
(11) Van Aalst Dennis (assistent), consult (1)
(7) Winnepenninckx Brigitte (assistent), consult (1)
(16) Maes Petra (assistent), consult (1)
(2) Kempeneers Nadine (medischeRegistratie), Opvraging MR buiten werkljst (2)
(16) Degol Ine (coassistent), studie (2)
(4) Van den Bogaert Saskia (assistent), consult (1)
(10) Beyens Hilde (supervisor), consult (1)
(4) Vaninbrouckx Koenraad (coassistent), mkg formulireem (1)
(1) Vandeborne Martine (administratie)
(4) Vanderschot Paul (supervisor), OOK DOOR MIJ GEOPEREERD! HIER IS IETS NIET IN ORDE!!!! (1)
(2) Ponette Diederik (assistent), consult (1)

Why need an overrule?

- System might not know yet that you will be involved in the treatment of this patient.
- Access granting can be quite strict: exceptions can be handled by overrule
 - Loose access control → no overrule needed
 - Strict access control → overrule option absolutely necessary

Remember: no information on paper!
- Structured overrule reasons
 - Code, not free text
 - Allows programmatic checking
 - E.g. if reason is “pre-anesthesia” → Check if patient received anesthesia soon after the overrule

Security risk prone patients



- “Secured patient”: all accesses are always logged
 - Overrule still necessary → system behaves as normal
 - Can not see difference with “normal” patient
- Extreme VIP cases: fake name
 - Dangerous! Might harm patient in an emergency

Procedure checking log

- IT only reacts to a request from mgmt or treating physician
 - Protect privacy of users
- List is first screened by treating physician(s)
- If unlawful access is detected → all overrules to other patients by that user are also screened
 - Gather more evidence that user is not trustworthy

Procedure checking log (2)

- Build up the case firmly
- Hunt down user(s)
- Torture
- Hang 'em (in public)

**A public hanging every now and then
does wonders for procedure compliance.**

Logs: developers

- System boys set up extra logs for developers (4 eyes principle)
- Changes to applications logs
 - Overrule log
 - Secured patients table
- System logs
 - Login and logout times
 - Tabel create, bcp, truncate, drop, grant for any database object

Developers can not remove the traces of their crimes without accessing these logs.

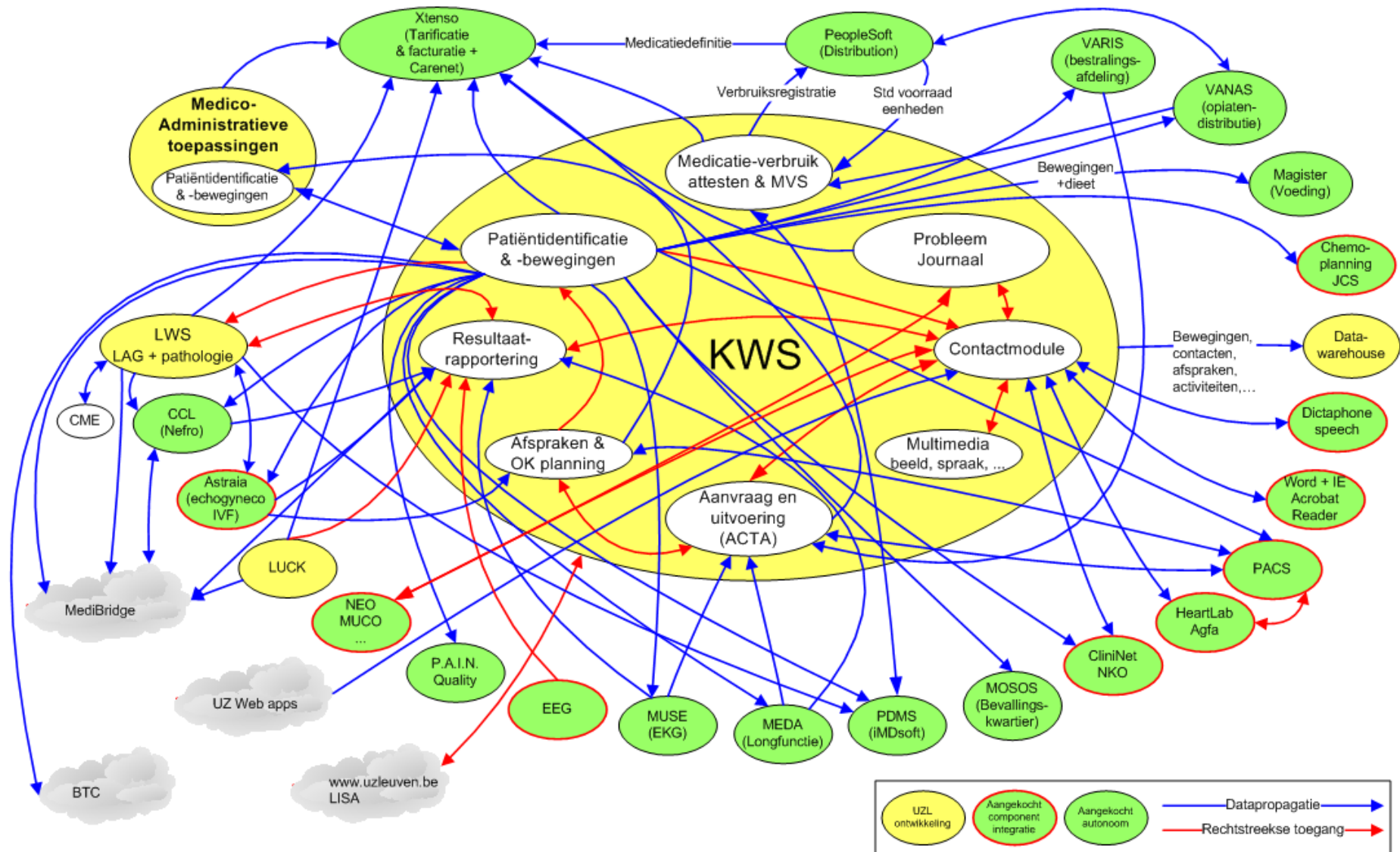
Problem: access control consistency over **ALL** applications

- Any hospital system will have several externally developed ancillary systems
 - Lab, Radiology (PACS), Chemotherapy, PDMS,...
- Data needed to deduce access rights
 - Too voluminous
 - Too volatile (causes many transactions on ancillary system)
- Rules
 - Too complex to implement
 - Too expensive to maintain
- Our (preferred) solutions:
 - **Front end component integration**
 - **Data propagation**

External parties:

- Not up to the task
- Not interested (unless €€€)
- Usually both

Clinical workstation integration & dataflows

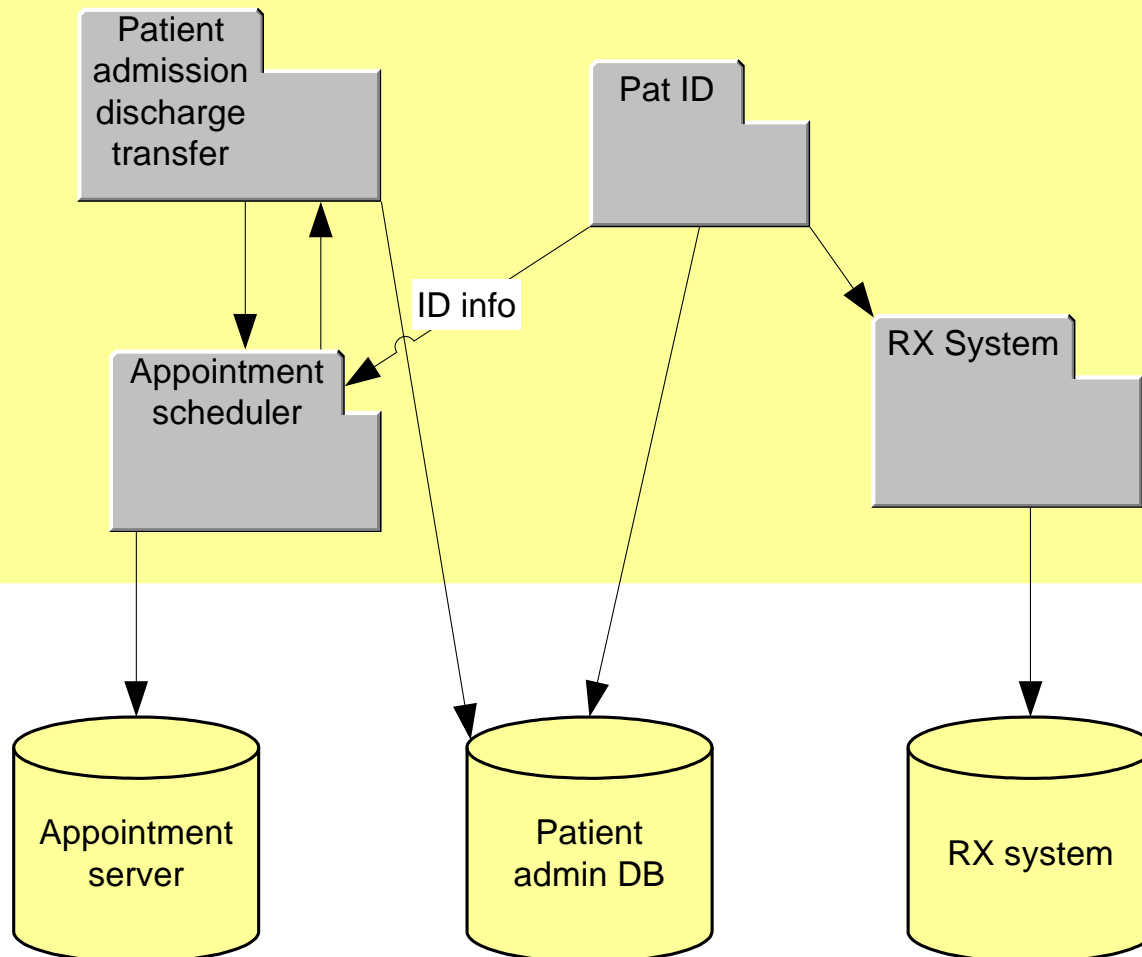


Front end component integration

- External application is embedded as a component within the clinical workstation
- To get to the component you need access on patient level (➔ CWS checks first, then passes control to external component)
- External component should be stripped from all functionalities that allows patient switching

Front end components

Medical file application



- Encompassing application governs:
 - access control to components
 - access control to patients
 - interaction between components
- Separate database per component or module
- No function replication necessary: the implementation of the logic (the component) is reused

Acties Dossier

Geriatric / A ▼ GER 0 hospitalisatie (difool/jflama0)

Con	Probleem	KBest	Waar	PO	ECG	VerwBrief	Attest	Beeld	Opname	Info
Acta	Afsp	MVer	Cics	Labo	Rx	Verw	Apo attest	Chemo	ZP	>>

Toon alles (3)

- U (2)
- c (1)

st	datum	activiteit	aanvraagInfo	boodschap	aantal	act
c	04-05-2004 00:00	Aanvraag kine bij gehosp. patient	test			925c
U	06-05-2004 14:49	Bloedname via port-a-cath			1	70251
U	06-05-2004 14:49	Therapeutische aderlating			1	70262

aantal rijen: 3

2 dagen terug

Aanvraag parameters:

Aanv: bart Van den Bosch Bart

Sup: jflama0

Planning: Dat 07-05-2004 00:00 Aanvr: 07-05-2004 12:46

Info:

Grid Boom

bld.per.	urine.st.	pl.perf.	tr.wondv	maags.pl	rx thor
bld.PAC	urDebOnd	transfus	ch.wondv	maags.dr	rx abd
	stoelgst	tz.inf.	aspirati	SV	FM NeuFy
	sputum	tz.HS	O2 ther.	BSplaats	nucl.gen
->Logies	uitstPAP		aerosol	BStoez	FM card
cons.cos	wisser	hygiene		BM ptie	FM pneu
rpl.	ander st	mobilit		LP	FM EndPn
pri.rpl	verb.mat	uitschei	=> cnsit	ascitEva	rxSkelet
proDeRpl		voeding	-> Kiné	scopieOK	RX

Vraag aan Voer uit Verbeter Verwijder Zender Toon Aanvraag Print Bon Nieuwe Lijst Sluit af Annuleer

Aanvraag

Uitvoer

Chemotherapy component in Clinical Workstation

Pt. - KWS-TESTPATIENT NUMMER 1 (1, 620829V999)

Acties Dossier

Geriatric / A ▼ GER 0 hospitalisatie (difoel/jflama0)

Con Probleem KBest Waar PO ECG VerwBrief Attest Beeld Opname Info
Acta Afsp MVer Cics Labo Rx Verw Apo attest Chemo ZP >>

Created on	Scheme	Department
10/12/2002	Cisplatinum-5FU (CDDP=100mg/m (V. 1)	DIGESTIEVE ONCOLOGIE
10/12/2002	Cisplatinum-5FU (CDDP=100mg/m (V. 2)	DIGESTIEVE ONCOLOGIE
12/12/2002	TEMODAL 150 mg/m ² (V. 2)	
08/04/2003	Cisplatinum-5FU (CDDP=100mg/m (V. 4)	
05/08/2003	CVP iv Hemato (V. 1)	
05/08/2003	CVP iv Hemato (V. 2)	
22/09/2003	ADRIAMYCINE 20mg/m ² (V. 7)	
22/09/2003	ADRIAMYCINE 75mg/m ² (V. 10)	
22/09/2003	CAF IV (V. 11)	
22/09/2003	CAF PO (V. 4)	
22/09/2003	CMF IV (V. 6)	
22/09/2003	CMF po (V. 20)	
22/09/2003	FEC IV (V. 10)	
22/09/2003	Navelbine (V. 1)	
22/09/2003	TAXOL 80mg/m ² wekelijks (V. 5)	

Prescriptions

Cycle	Created	Administered on
I-1	22/09/2003, 15:23	Administered on 22/09/2003, 00:00
I-8	22/09/2003, 15:24	Administered on 22/09/2003, 00:00

aantal rijen: 97

Slide 42 of 01

Prescription I-1

File Tools

Prescription information

Cycle: I-1 Created on: 22/09/2003, 15:23
Prescribed on: 22/09/2003, 15:23 Administered on: 22/09/2003, 00:00

Chemo Form information

Created on: 22/09/2003, 15:23
Department: DIGESTIEVE ONCOLOGIE
Scheme: CAF IV
Scheme version: 11 Date: 2/08/2003

General Patient Actions Variables Errors/Warnings

Unit:

Prescribing physician: Aerts Rita

OG. NR. Prescribing physician:

Activity index: 0

Remark:

Pl. - KWS-TESTPATIENT NUMMER 1 (1, 620829V999)

Acties Dossier Geriatrie / A ▼ GER 0 hospitalisatie (difool/jflama0)

Con Probleem KBest Waar PO ECG VerwBrief Attest Beeld Opname Info
Acta Afsp MVer Cics Labo Rx Verw Apo attest Chemo ZP >>

Episode 1 9-feb-2004 : Infertility

Patiënt: 5262, NUMMER 1 KWS-TESTPATIENT, DOB 29-aug-1962, age 41

Samenvatting

Patient Demographics

Case information

History - Female

History - Male

Personal History - Male

Previous sperm analysis

Female clinical

Male clinical

Counselling

Staff

Contracts

Treatment

Stimulation

Follicle Tracking

IVF / ICSI

d-1 - Preparation

d0 - Oocytes

Thawing

d1

d2-6 - ET

Embryo scoring

IUI

Sperm Data

Treatment

Start hMG/FSH

Pituitary inhibition

Stimulation

Medication (Ant)agonist

Treatment Fertility Centre

BELRAP no.

Treating clinician

Weight kg

Contact patient

Follicle Tracking

LMP Injection time Lab telephone

Date of cancellation Cancellation cause

Appointment partner Ovulation trigger Total dose of Gonadotrophins

Date	day	E2	Prog	LH	FSH	hCG	EM	>14mm	Dose M	Dose A	Time app.	Action
1												

get lab data

20												
19												
18												
17												
16												

F1 - help F2 - summary F3 - navigator F4 - expand screen F7 - graph F8 - all graphs F9 - measurements F10 - close

Data propagation

- Relevant data from ancillary system is propagated to the Clinical Workstation DB.
- No access from outside the dept to the anc system

 Load on local system lower

 Tight access control

 Separate data model to be maintained

 Viewer needed if non text data

Integrity: digital signatures

- Why not use digital signature using the Belgian eID card (BelPIC)?
- User assures himself of the integrity of the data
- IT people can not tamper with the data
- You payed for it, you might as well use it
- BUT....

“Issues”

- You don't see what you sign.
 - Something is being signed
 - Is what you see on screen what you really sign?
- **You have to trust the application**
- How many docs do you sign?
 - Application asks PIN code for EVERY signature

**This is of paramount importance when using BelPIC:
you are personally (as a citizen, not as an employee)
responsible for what you sign.**

Wear on BelPIC

- BelPIC estimated life of 25.000 signatures
= 5.000 per year (new card every 5 years)
= boils down to 23 signatures/day!
- More than adequate for private use,
not for professional clinical use!
- Quid costs and temporary impossibility to sign
due to defunct BelPIC?

Costs (2005)

- Readers
 - Reader in keyboard (extra) €27
 - Separate reader €29
 - Separate reader with num pad €115
- Installation and maintenance
- Software development
- **User time:** extra seconds per transaction!
 - Inserting card: X seconds
 - Keying pin code: 2-3 seconds
 - Signature calculation: 2 seconds

Questions

- Is the safe usage of the BelPIC signature **ergonomically** feasible in a clinical setting?
- Does it legally make sense to use a digital signature in a more ergonomic but less secure way (sacrificing non-repudiation)?
- Can an employee refuse to use his personal BelPIC for professional purposes because of the (however unlikely but) possible misuse where he might be implicated as a person?

Alternatives?

- Separate professional digital signatures from personal ones (separate professional ID card)
- Electronic timestamping
 - Does ensure integrity in time and secures the time when the data was available, but not non-repudiation for the user that inserted the data
 - Can be done without ergonomic cost
 - Time at which a result was in, updated,... often very important.
 - Fraud occurs almost always after the facts: timestamp reveals tampering

Remember

Security is the reciprocal of convenience

-- Netvision > Ubizen > Cybertrust > Verizon

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

-- Bruce Schneier (auteur Blowfish)

The user is going to take dancing pigs over security every time.

-- Bruce Schneier (auteur Blowfish)