Dataprotection in Hospitals

Bart Van den Bosch
CIO UZ Leuven
March 4, 2008
Dataprotection

• Situation of hospital data protection
• (Fysical security)
• System data protection
  – Availability & Integrity
  – Confidentiality
• Network security
• Application level data protection
Situation

• 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.
13th Annual HIMSS Leadership Survey 2002
Top concerns security electronic patient records:

- Patients' Lack of Confidence: 19% (2001) vs 29% (2002)
- Don't Know: 2% (2001) vs 5% (2002)
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.

Data protection – Bart Van den Bosch
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)

Δ 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

Data Center 1
- SQL Server
- Sybase
- FAS960c
- FAS3020c
- FAS3070mc
- GX name space
- Snapshot/Snapmanager
  - Hourly
  - Daily
  - Weekly
- NearStore

Data Center 2
- SQL Server
- Sybase
- FAS960c
- FAS3020c
- FAS3070mc
- GX name space

Data Center 3
- SQL Server
- Sybase
- FAS3070mc
- GX name space
- NearStore

.log shipping

syncmirror

snapvault
Replication of a database

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

Transfer process

Primary computer

Database

Log

Log of all changes

Stand by computer

Copy of the database

Holds all data (with a small delay)
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 ± 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
Confidentiality (database level)

• 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
Authentication

• 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

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...

<table>
<thead>
<tr>
<th>Patients</th>
<th>Report</th>
<th>Validation</th>
<th>Activities</th>
<th>Appointments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physician</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Supervisor</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Nursing</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Administrative</td>
<td>●</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

(In many systems this axis is not used)
Fine grained access control

• “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
Logs: data level

- 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
File is locked

→ system can not deduce a relationship between user and patient
“You do not have access. Please supply a valid reason. Warning: It is a serious misdemeanor to access data without a valid reason. The reason you supply will be checked.”
Automatic popup when opening patient file. Disappears automatically after a few seconds (or by closing it)
Automatic popup when opening patient file. Disappears automatically after a few seconds (or by closing it)
The popup shows an overview of the last 100 overrules grouped by user. For each overrule where a reason was given, the number of times this reason was used.

<table>
<thead>
<tr>
<th>Number of overrules</th>
<th>User’s function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Coels Maarten</td>
</tr>
<tr>
<td></td>
<td>Delinder Pieter</td>
</tr>
</tbody>
</table>
On clicking the popup a list is given with details of the overrules.
Clicking this button displays the popup again.
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
• 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
  – Table 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

Data protection – Bart Van den Bosch
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

- 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

Data protection – Bart Van den Bosch
Chemotherapy component in Clinical Workstation

Data protection – Bart Van den Bosch
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)