



Presenter Names: Merv Matson,  
RightsMarket Inc

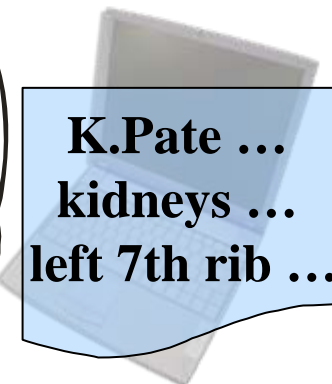
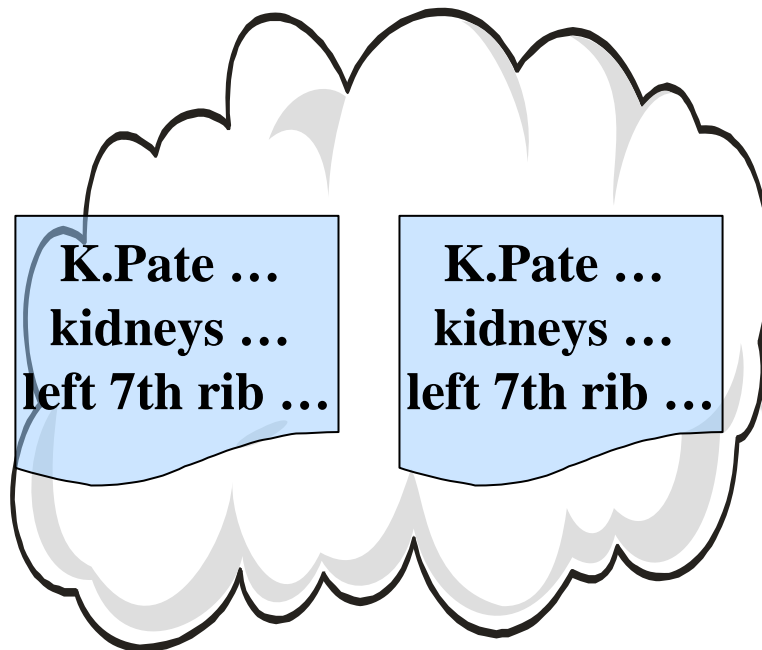
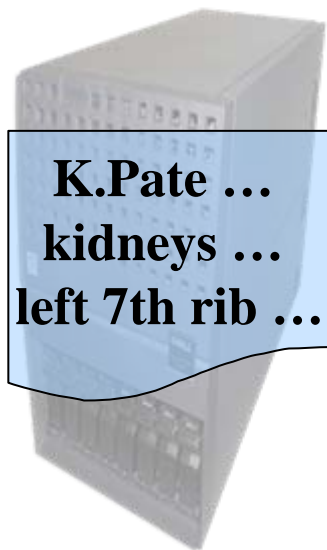
Topic: A policy engine for granting access to  
persistently secure EHRs

Track: Health Information Protection:  
Privacy and Security

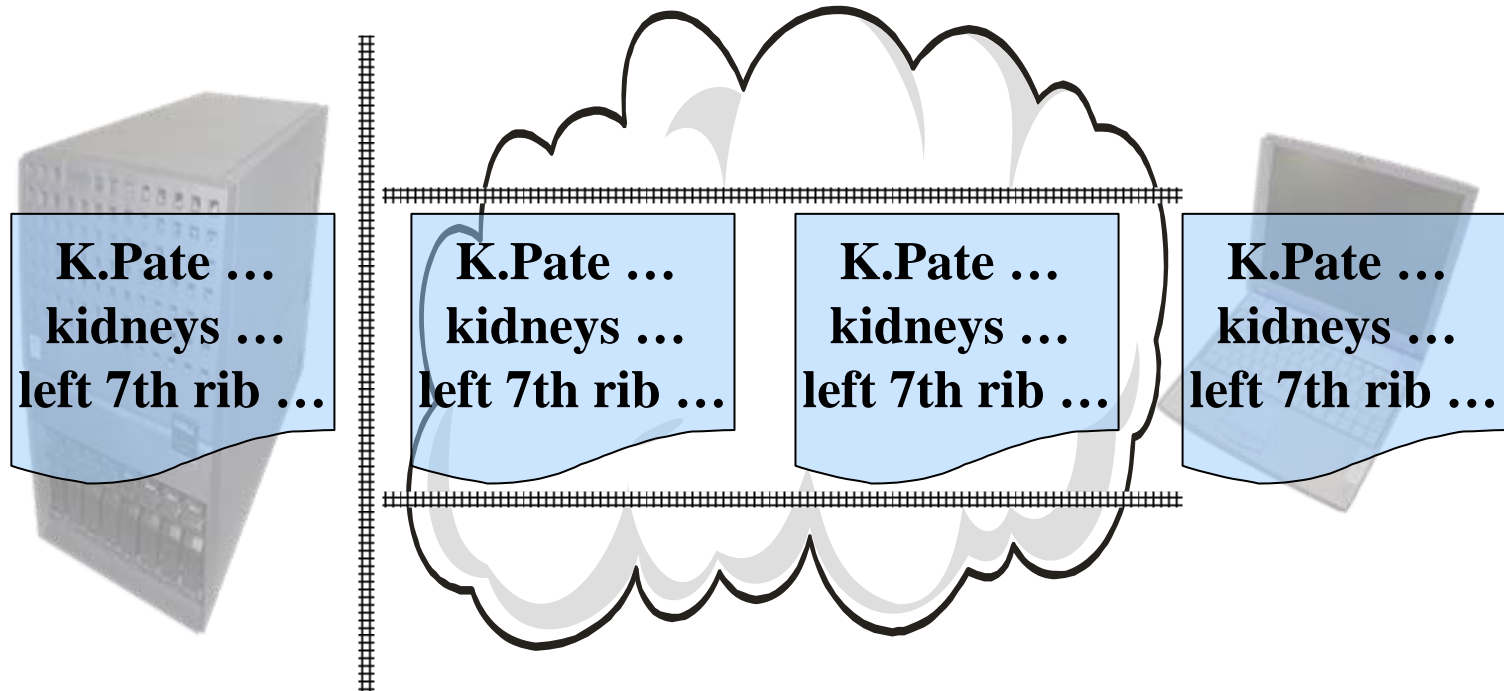
# Outline A policy engine for granting access to persistently secure EHRs

- **Persistently secure EHRs**
  - Contrast with repository and delivery security
  - Security is inherent, all use is authorized and tracked
- Granting access (or permission or entitlement)
  - Persistent security enables sharable EHR
  - Challenge: how does legitimate user get permission?
- Policy engine
  - The Policy and Peer Permission (PPP) system
    - Authoring and interpreting policy for granting permission to the distributed EHR
  - The PPP project

# EHR Use - computer file transfer



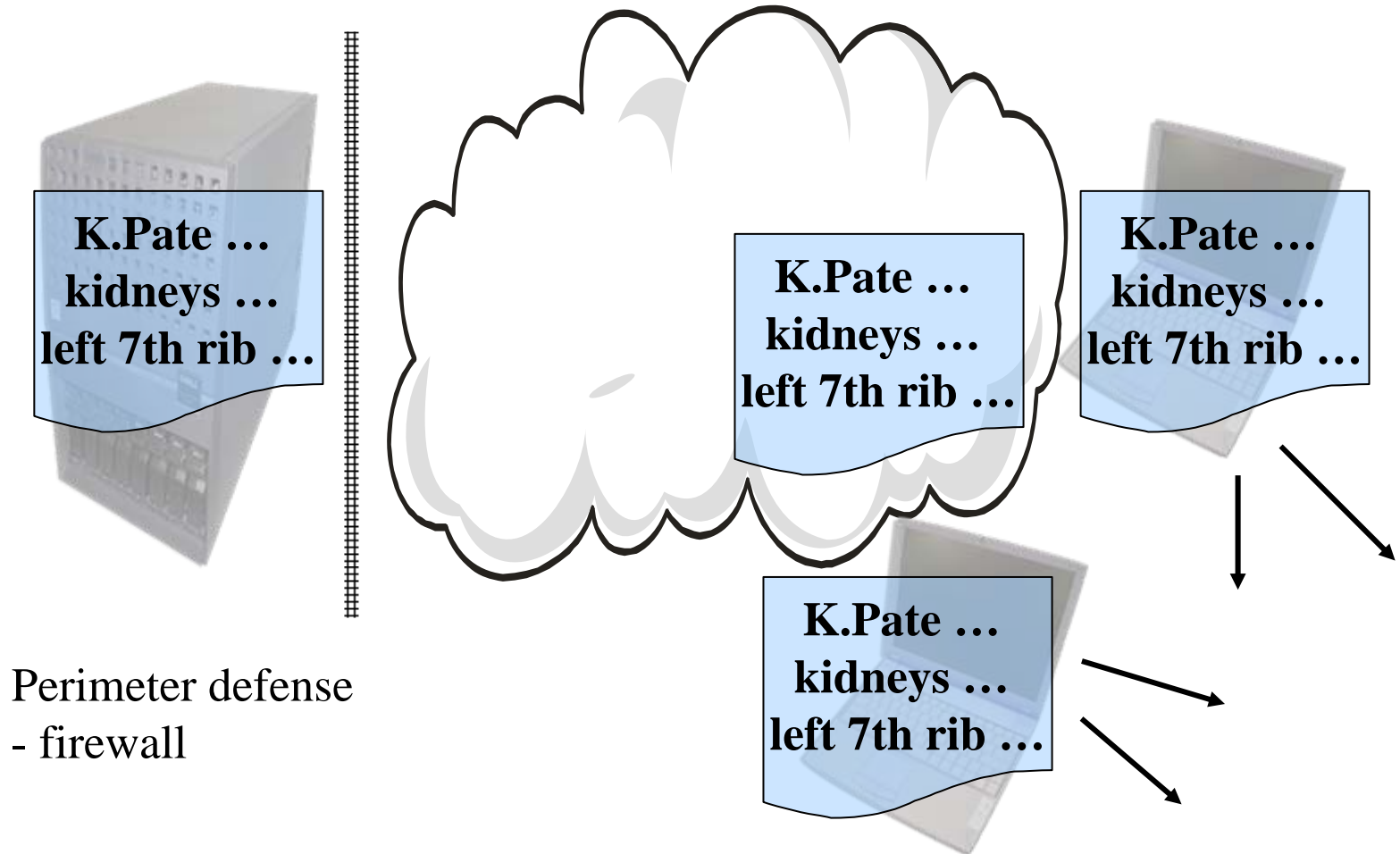
# EHR Use - defenses



Perimeter defense  
- firewall

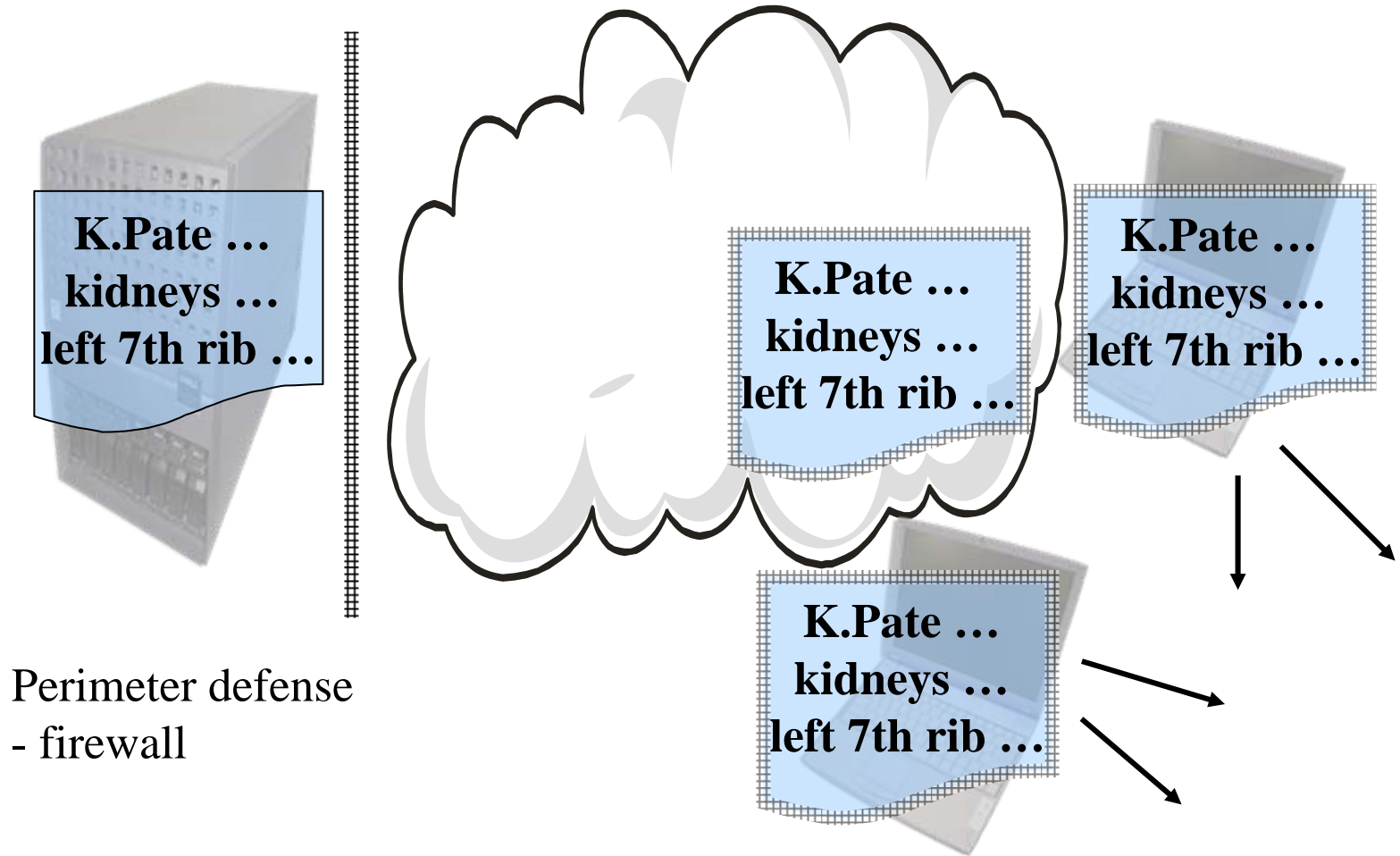
Network defense  
- tunnel

# EHR Use - defenseless outside

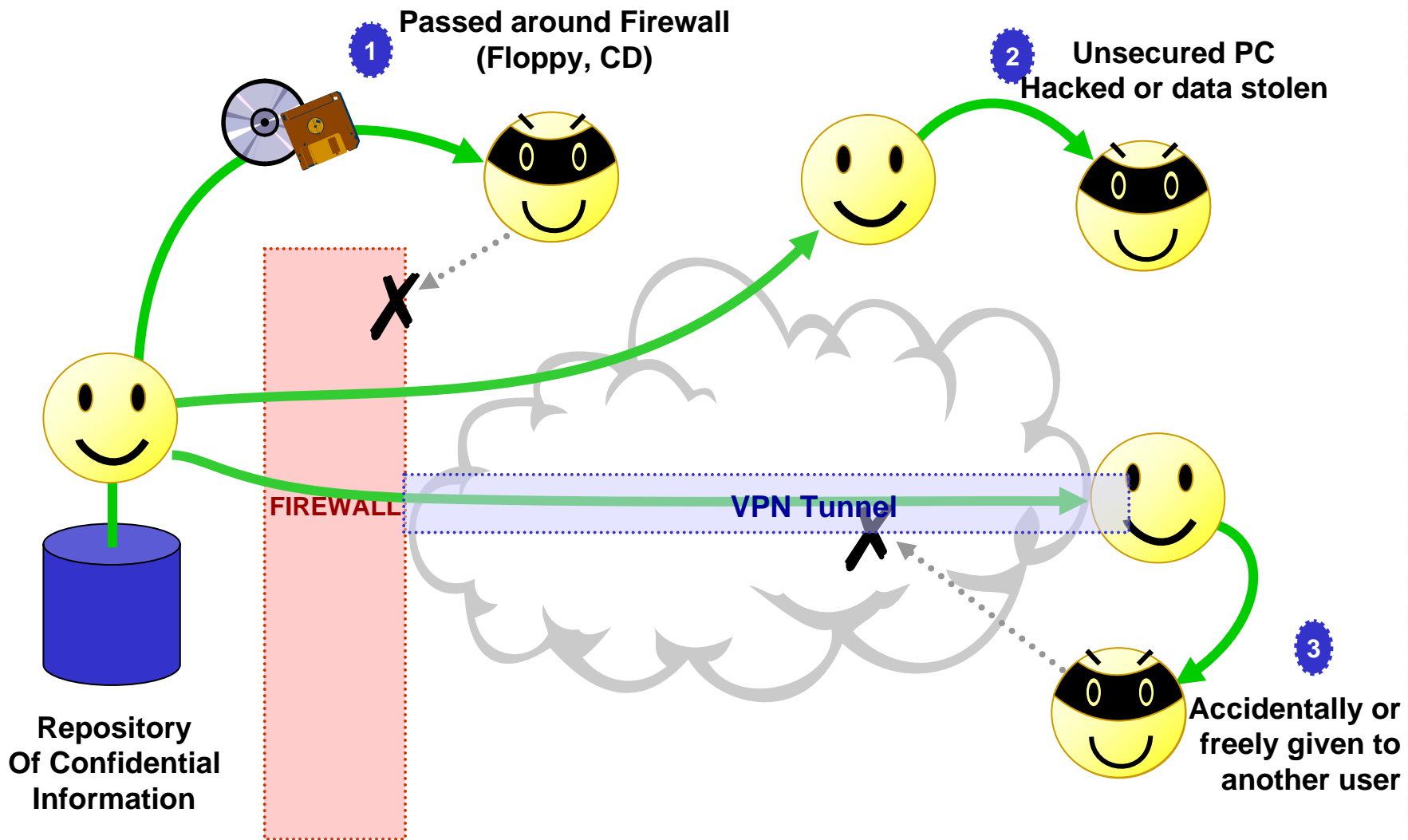




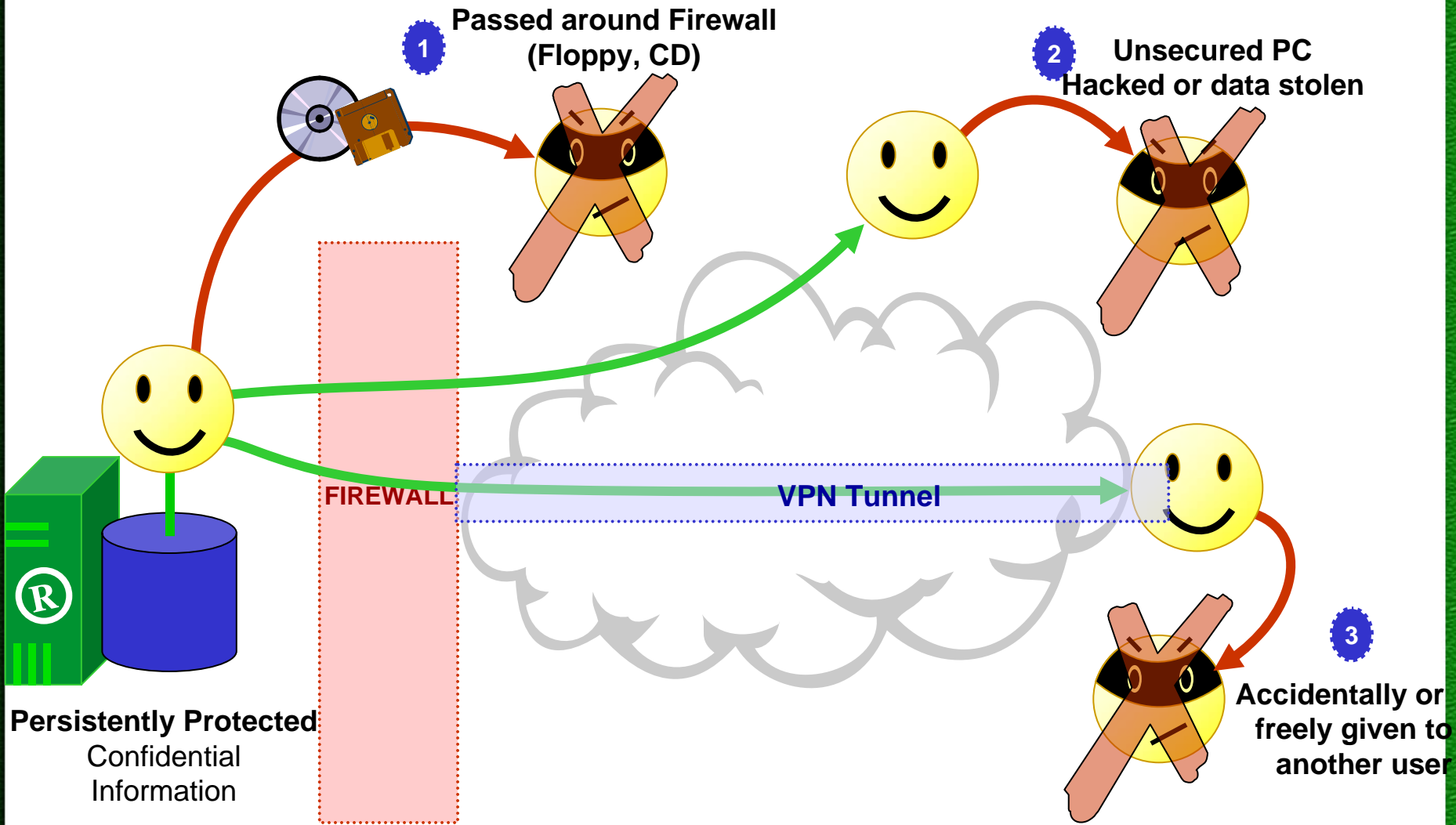
# EHR Use - protected everywhere



# Without Persistent Security



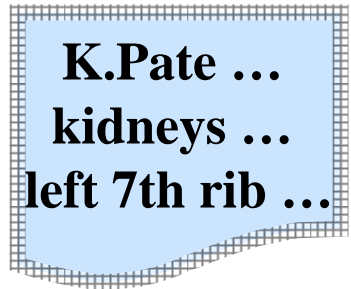
# With Persistent Security





# Persistent Security: Defn, Effects

- Technology for implementing inherent protection
  - Adapted from the eCommerce of eBooks
- Protection is inherent in the record
  - Never an unprotected copy of the EMR
    - Even outside the repository perimeter defense (firewall) and the network delivery defense (VPN tunnel)
- Every use of the EMR is authorized and tracked
  - Even peer-to-peer pass-along use
  - Even offline (off-network) use



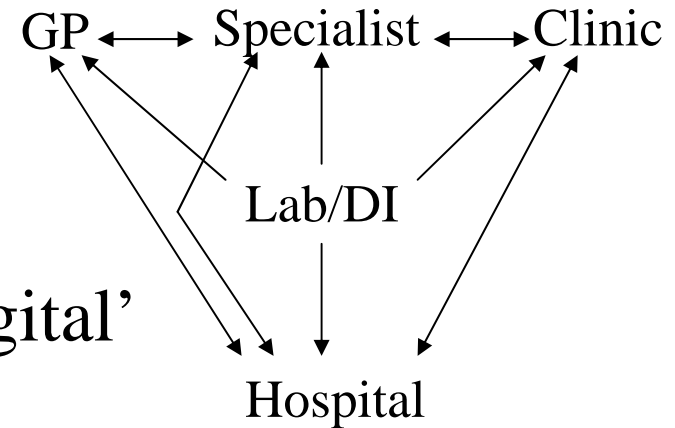
# Outline A policy engine for granting access to persistently secure EHRs

- Persistently secure EHRs
  - Contrast with repository and delivery security
  - Security is inherent, all use is authorized and tracked
- **Granting access (or permission or entitlement)**
  - **Persistent security enables sharable EHR**
  - **Challenge: how does legitimate user get permission?**
- Policy engine
  - The Policy and Peer Permission (PPP) system
    - Authoring and interpreting policy for granting permission to the distributed EHR
  - The PPP project

# Shareable EHR

- There are many sources, custodians, repositories and points of use of the distributed MR.

- Persistent security enables
  - Current EMR custodians to maintain custody as we ‘go digital’
  - Referral process, hospital admittances, care relationships , ... , to determine distribution and sharing of the EHR
- BUT ...



# Challenge: granting permissions

- How does the legitimate user get permission in this many to many to many relationship?
  - Many patients, each with many EMRs
  - Many potential legitimate care givers
- Coarse permissions policy? If you can get at any EMR in the repository you can get at all.
- Fine, one to one, explicit assignment?
- Automatically interpreted policy with peer permission transfer; all tracked.

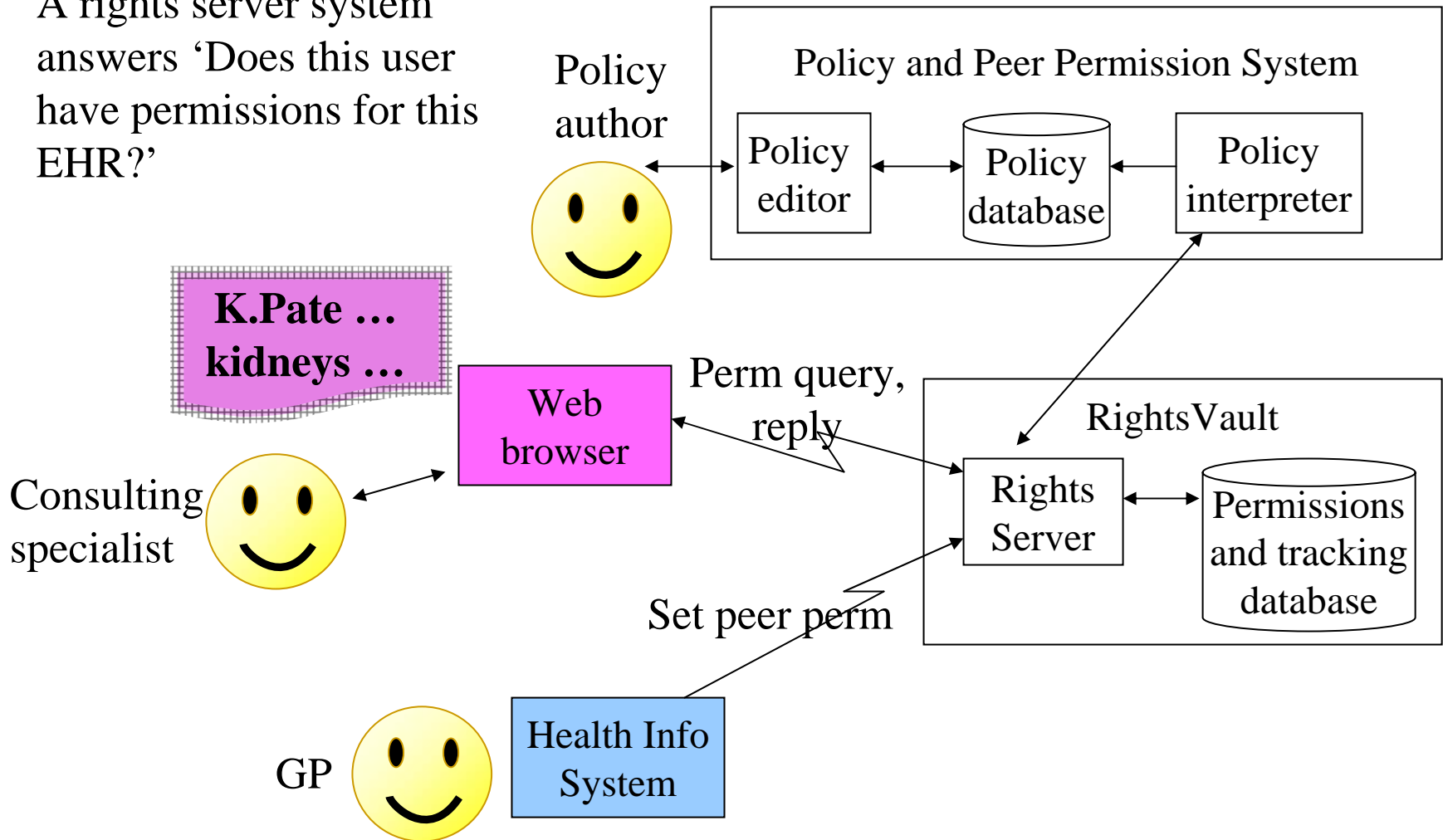


# Outline A policy engine for granting access to persistently secure EHRs

- Persistently secure EHRs
  - Contrast with repository and delivery security
  - Security is inherent, all use is authorized and tracked
- Granting access (or permission or entitlement)
  - Persistent security enables sharable EHR
  - Challenge: how does legitimate user get permission?
- **Policy engine**
  - **The Policy and Peer Permission (PPP) system**
    - **Authoring and interpreting policy for granting permission to the distributed EHR**
  - **The PPP project**

# Policy & Peer Permission System

A rights server system answers 'Does this user have permissions for this EHR?'



EMR

X-Ray Rep  
Cumulative I

ER Visits  
Medications

Scheduler

Save Report As File:



File Na

PateXr

Sen

✉ PateXray.pdf - Message (HTML)

Send Save Print Copy Paste Undo Redo Forward Backward Bold

File Edit View Insert Format Tools Actions Help

To: Dr. Mary Spencer

Cc:

Bcc:

Subject: PateXray.pdf

Dear Mary.

Please give my your opinion regarding the case we discussed this morning.

I have granted you rights to view EMR  
[www.Genner.RightsVault.com/PateXray.pdf](http://www.Genner.RightsVault.com/PateXray.pdf)  
for 2 days from now.

Regards, Bill

There is satisf  
increased activ  
other abnorma  
facet joint. Mil

Findings are ot

REPORT DETAILS

t: PATE, KEVIN M

mild  
ir  
cent

.pdf

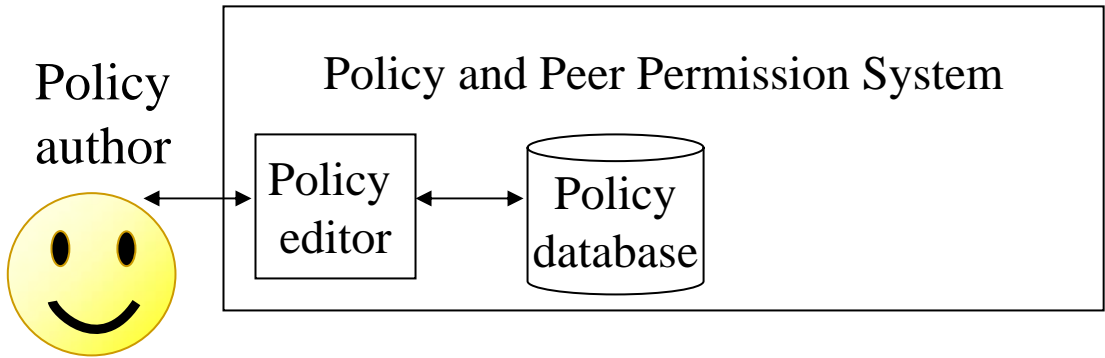
# Policy Statement Examples:

- My Family Physician may read and print all of my personal health information.  
Exception ...
- Referral Policy: The consulting specialist assigned to me at Consulting Hospital may read all of my medical records needed for my consultation.
  - Policy based on impending care relationship



# How is it done?

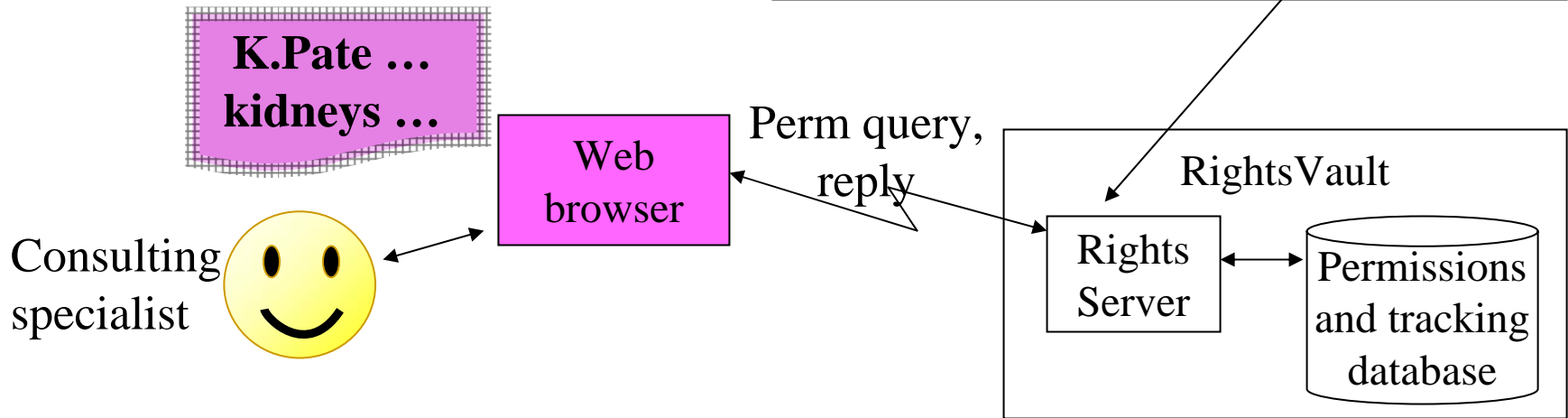
Write policy in  
user-friendly  
language,  
translate to  
machine  
interpretable,  
store in policy  
database



The consulting specialist assigned to me at Consulting Hospital may read all of my medical records needed for my consultation

# How is it done?

Interpret policy  
from database as  
record is used.



# Write a policy: select, edit, new

default - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <http://dravais1/RulesWizard/SelectRule.aspx> Go Links >>

|                        |                      |   |
|------------------------|----------------------|---|
| <a href="#">Select</a> | <a href="#">Edit</a> | Create a Patient or Care Giver grouping (i.e., a Ward)                  |
| <a href="#">Select</a> | <a href="#">Edit</a> | Associate a patient to a grouping                                       |
| <a href="#">Select</a> | <a href="#">Edit</a> | Associate a General Practitioner to a grouping                          |
| <a href="#">Select</a> | <a href="#">Edit</a> | Associate a Primary Care Giver to a grouping                            |
| <a href="#">Select</a> | <a href="#">Edit</a> | Provide Primary Care Giver entitlements for a Patient                   |
| <a href="#">Select</a> | <a href="#">Edit</a> | Pass entitlement from one Care Giver to another with a time limitation  |
| <a href="#">Select</a> | <a href="#">Edit</a> | Provide EMR access to Care Givers associated to a grouping              |
| <a href="#">Select</a> | <a href="#">Edit</a> | Assign explicit PCG access rights to EMRs in a Ward limited by duration |
| <a href="#">Select</a> | <a href="#">Edit</a> | Restrict EMR access in a Ward   |
| <a href="#">Select</a> | <a href="#">Edit</a> | GP's from a Hospital can print Patient Records for Hospital             |

New Rule

Local intranet

arket

# Write policy: edit

NewRule - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://dravais1/RulesWizard/EditRule.aspx?Rule=24>

Rule with substitution tokens:

PCG \_\_PCG\_\_ has \_\_Right\_\_ access to EMRs in \_\_GROUP\_\_ for \_\_DAYS\_\_ Days

Description of the rule (no substitution tokens):

Assign explicit PCG access rights to EMRs in a Ward limited by duration

Rule Script:

Validate Script Update Rule

[Return to Rules](#)

Available Tokens

|              |                      |
|--------------|----------------------|
| __CG__       | Care Giver           |
| __DAYS__     | days                 |
| __GP__       | General Practitioner |
| __GROUP__    | Group                |
| __LINK__     | Link to Parent Rule  |
| __NEWGROUP__ | Group                |
| __P__        | Patient              |
| __PCG__      | Primary Care Giver   |
| __RIGHT__    | Use Right            |

Done

Start Windows ... Inbox - Mi... SQL Serve... PPP Rules ... NewRule ... Local intranet 5:31 PM



# Policy and Peer Permission Project

- eBooks to EHRs
- From 2002-Jan-09 to Dec-19
- 600k\$ development project, half funded by CANARIE's E-Health / Telehealth program
- Deliverables
  - Software: policy editor, policy interpreter
  - Policy: starter set of policy statements for alpha test

# Policy and Peer Permission Project

| <b>Participant</b>  | <b>Role</b>        | <b>Principal Investigators</b>       |
|---|--------------------|--------------------------------------|
| UCalgary Telehealth<br><a href="http://www.ucalgary.ca/telehealth">www.ucalgary.ca/telehealth</a> | Policy researcher  | Dr. Maryann Yeo<br>Dr. Penny Jennett |
| UOttawa Heart Institute<br><a href="http://www.ottawaheart.ca">www.ottawaheart.ca</a>             | Alpha test site    | Dr. Shu-Tim Cheung                   |
| RightsMarket Inc<br><a href="http://www.RightsMarket.com">www.RightsMarket.com</a>                | Software developer | Merv Matson                          |
| CANARIE<br><a href="http://www.canarie.ca">www.canarie.ca</a>                                     | Funder             | Wendy Zatylny                        |

# How do we get to 'sharable'?

Leave custody of records with current custodians as they go electronic

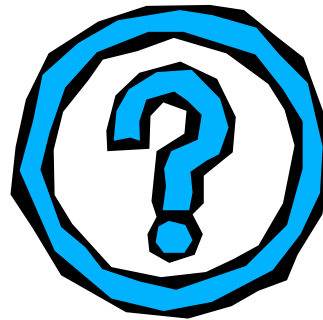
- Go **persistent**: answer the need for security at the point of use of the records, wherever that is
- Let custodians control use of persistently secured records with **policy and peer permissions**
- Make it easy for individual care givers to get started with **minimal infrastructure and buyin**; Let the early adopters of electronic records pull in the rest by demonstrating advantage

# Summary    A policy engine for granting access to persistently secure EHRs

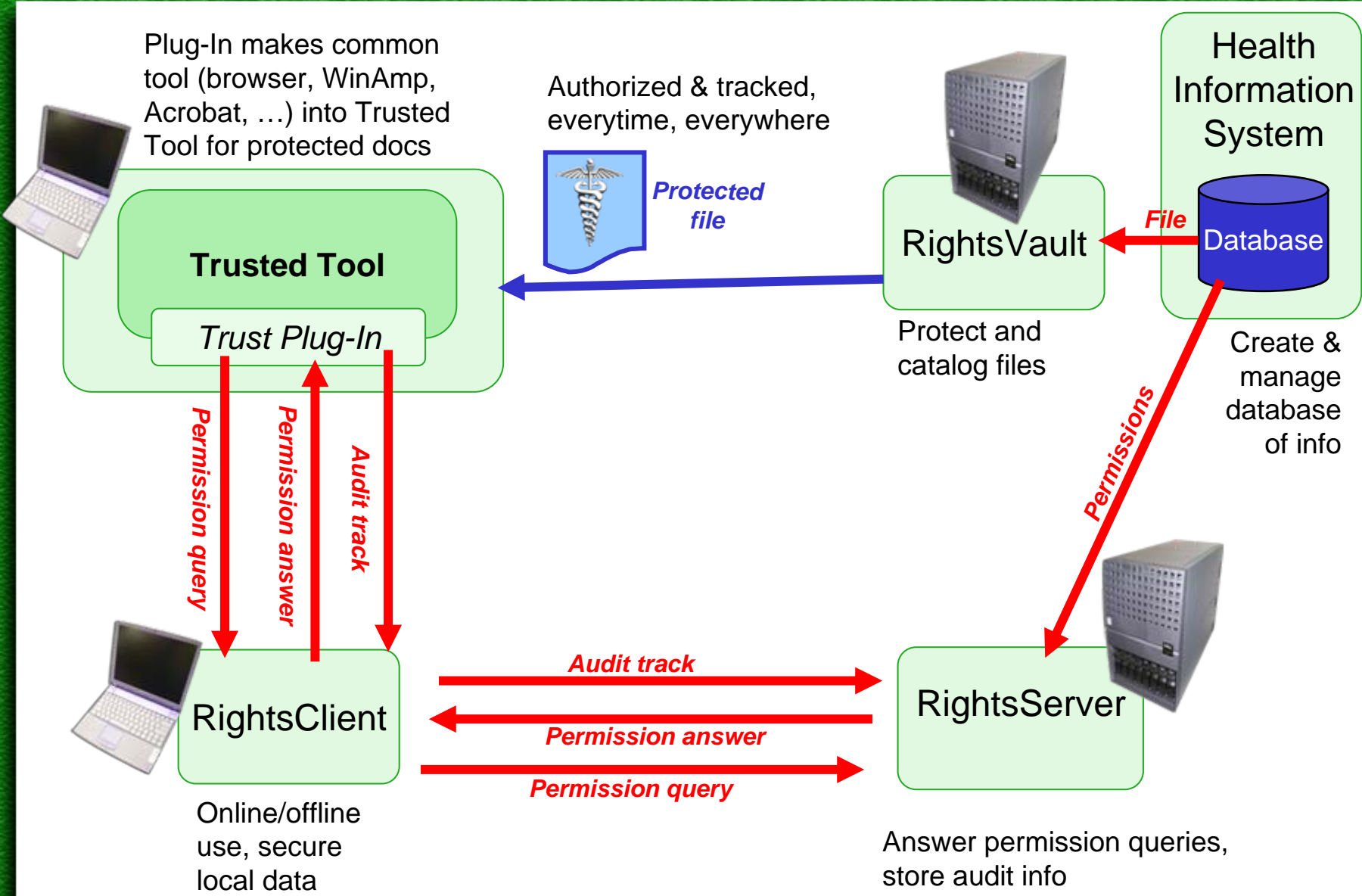
- We have persistent security now
  - Not widely known in confidential records applications; Deployed in eBooks eCommerce
- Need policy & peer system for granting access permission to persistently secure EHRs
- PPP project will build and test-deploy the Policy and Peer Permission system
- [www.RightsMarket.com/RightsVault/PPP](http://www.RightsMarket.com/RightsVault/PPP) tracks progress of project



# Questions ?



Supplemental slides for  
anticipated questions



- Home
- Solutions
- Demo
- Corporate
- Contact Us

- Overview
- RightsPublish
- RightsVault
- Systems Integration
- How it Works
- Customer Sites
  - ASTD
  - Canadian Broadcasting Corporation
  - Fifth Era
  - Janyce Bell
  - KymWorld
  - Giuridica Edinform
  - Meducational Publications Unbound
  - Systems Thinking Press
  - Terrorism Books

Quick Links

PDF RightsPublish Brochure, 328K



# RightsMarket

digital rights management.

- Ideas
- Quirks & Quarks
- The House
- As It Happens

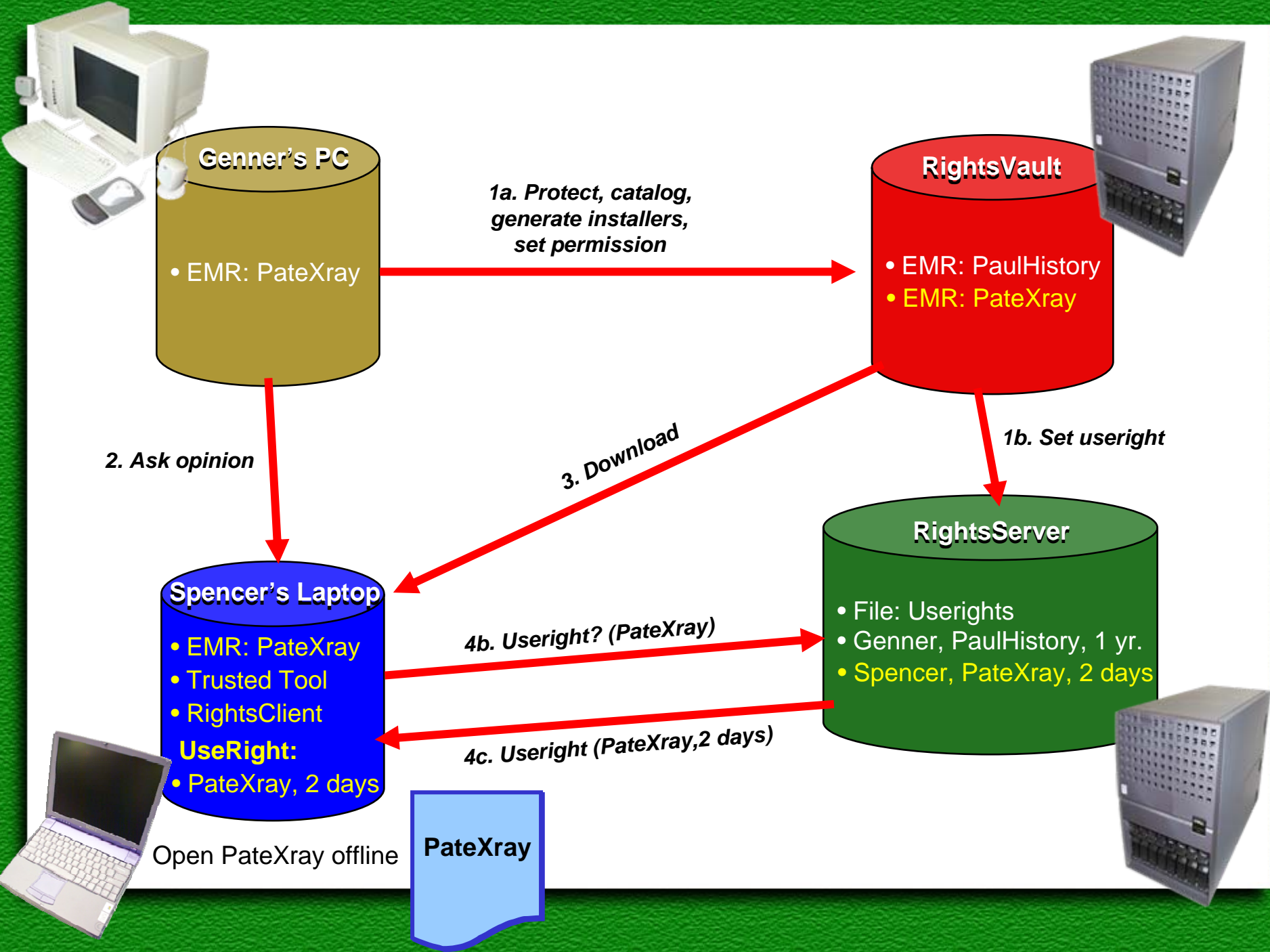
rights management, RightsMarket offers Systems Integration (SI) services that use our market technology to provide custom solutions tailored to our clients' needs.

and services to  
**manage**  
 and  
**distribute**  
 digital content.

Our services to securely distribute digital content and prevent piracy. Offering solutions for both text and audio in the areas of music, film, and television, RightsMarket enables organizations to capitalize on the benefits of digital distribution over the Net.

The company's flagship product, RightsPublish, is an end-to-end solution for selling, securing and tracking digital content. Easy to implement, RightsPublish provides a Web storefront, eCommerce, complete audit trail, and persistent security. See how RightsPublish can work for you. Our 90 day business validation program offers you an opportunity to try out our products and services at a minimum cost.





# Electronic Medical Record Audit Trail

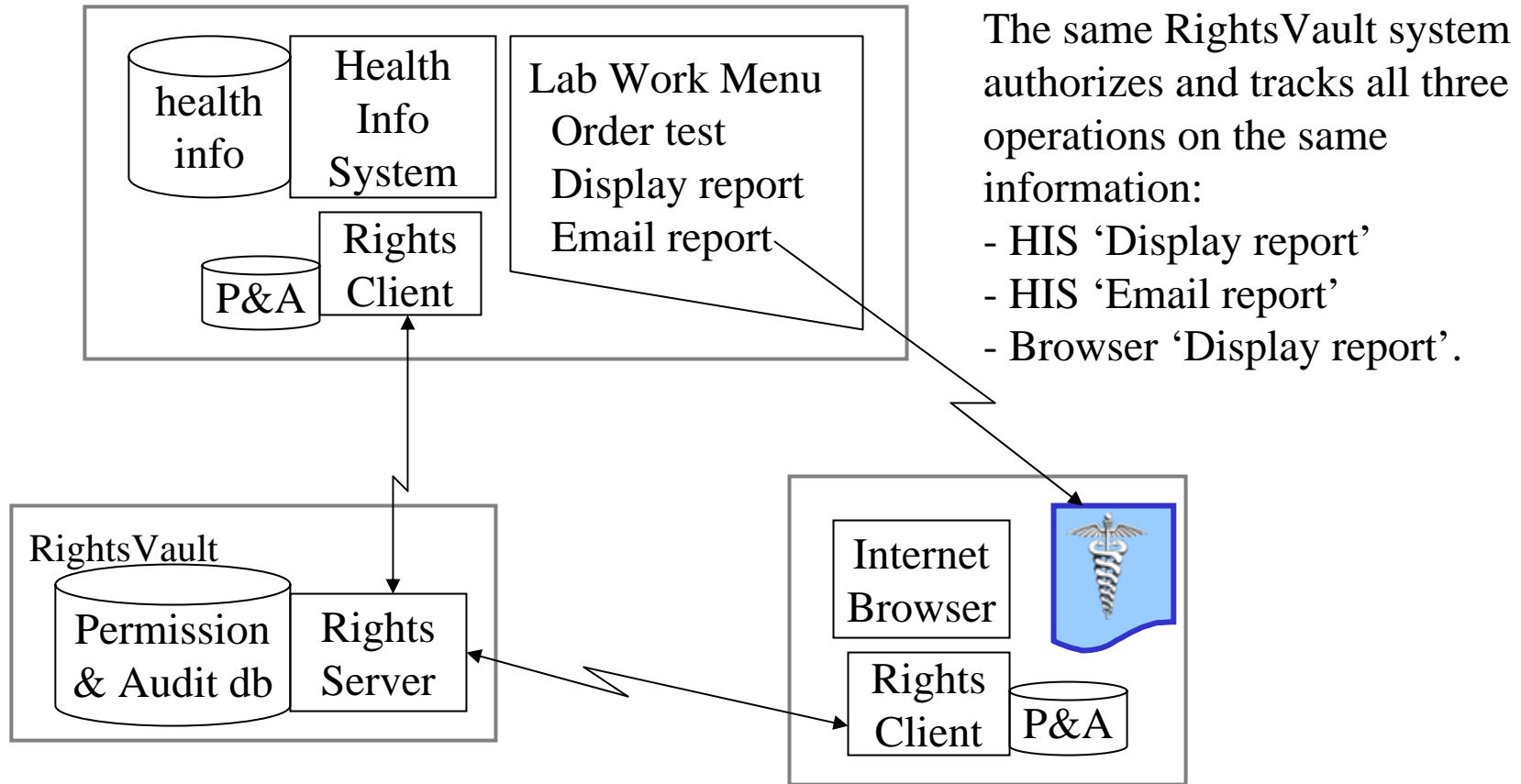
For Dr. William Genner, Id 098765

Date 2001-11-10

Criteria Patient: Kevin M. Pate, Id 123456789; Records: File PateXray.pdf

| EMR      | Activity | By                | When                | Details                         |
|----------|----------|-------------------|---------------------|---------------------------------|
| PateXray | set perm | 098765<br>Genner  | 2001-11-08<br>13:07 | 132457; read, 2 day<br>from set |
| PateXray | open     | 132457<br>Spencer | 2001-11-08<br>15:33 | close 2001-11-08<br>15:36       |
| PateXray | open     | 132457<br>Spencer | 2001-11-08<br>19:13 | close 2001-11-08<br>19:26       |

# Integrated Authorization and Tracking



# Conclusion

*Persistent security and complete use tracking*  
not just *delivery security and check-out tracking*.

*For more information*

[www.RightsMarket.com](http://www.RightsMarket.com) > Solutions > RightsVault  
> Solutions > Customers > CBC  
> Demo

Merv Matson      MatsonM@RightsMarket.com      (403) 571-1836



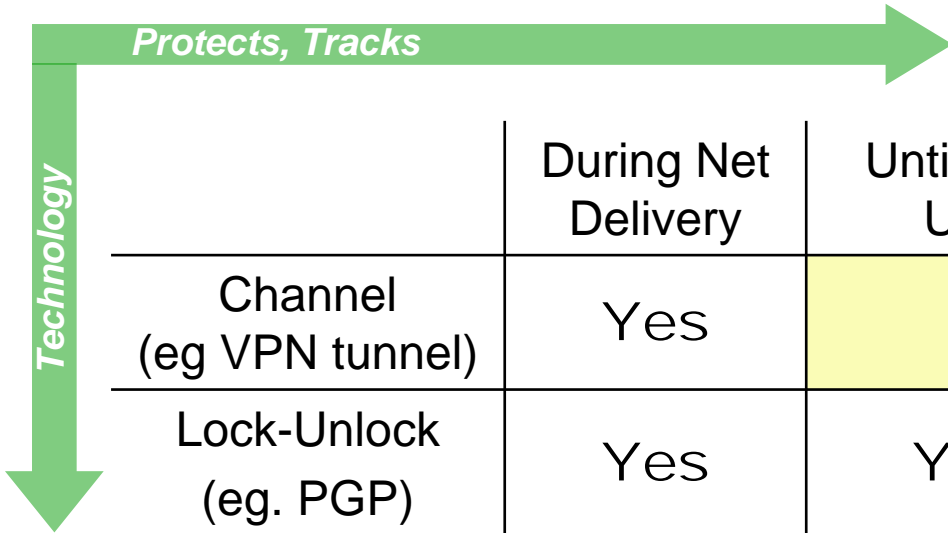
# Security – Risk Model

|          |                 | Security Strength                   |                        |        |
|----------|-----------------|-------------------------------------|------------------------|--------|
|          | Attack, Risk    | VPN                                 | Persistent             |        |
| Location | Authentication  | Strong <sup>1,2</sup>               | Light <sup>3,4</sup>   |        |
|          | At Host System  | NA <sup>5</sup>                     | NA/Strong <sup>6</sup> |        |
|          | In Net Transit  | Strong                              | Strong                 |        |
|          | At Point of Use | Hack attack; carelessness; mischief | NA <sup>5</sup>        | Strong |
|          |                 |                                     |                        |        |

1. Independent certification authority
2. Even stronger if two factor identification employed
3. Operator acts as own certification authority
4. But compatible with VPN
5. But compatible with Persistent
6. If employed at the host database system (probably not)

# Not Just Delivery Security

## *EMR Security & Use Tracking*



|                            | During Net Delivery | Until First Use | Everytime, Everywhere |
|----------------------------|---------------------|-----------------|-----------------------|
| Channel<br>(eg VPN tunnel) | Yes                 |                 |                       |
| Lock-Unlock<br>(eg. PGP)   | Yes                 | Yes             |                       |
| Persistent                 | Yes                 | Yes             | Yes                   |

# Built on ‘Authorize and Track’

*every time, everywhere*

## **RightsPublish**

Web-based, end to end service to publish valuable digital property; eBooks & eMusic

## **RightsVault**

Integratable subsystem to persistently secure confidential/private digital records; *eg. Medical docs & audio transcripts*

## **RightsCore**

Digital Rights Management (**DRM**) platform to secure digital objects, authorize and meter/track/audit their use, supporting offline and online use

## **The Internet**

Copy and distribute digital objects, worldwide, point-to-multipoint, nearly instantaneously, nearly free.

# PIPEDA - Accountability

- An organization is responsible for personal information under its control and shall designate an **individual** or individuals who are **accountable** for the organization's compliance
- An organization is responsible for ... information that has been transferred to a third party for processing. The organization shall use **contractual or other means** to provide a comparable level of protection while the information is being processed by a third party.



# PIPEDA - Safeguards

Personal information shall be protected ...

- ... protect personal information against loss or theft, as well as **unauthorized access, disclosure, copying, use, or modification** ... regardless of the format ...
- The methods of protection should include
  - (a) physical measures ... locked filing cabinets ...
  - (b) organizational measures ... security clearances ...
  - (c) technological measures ... use of passwords and encryption.

Authorize Use, every time, everywhere

# PIPEDA - Individual Access

- ... the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

Track Use, every time, everywhere