2002-04

A Policy Engine for Granting Access to Persistently Secure EHRs

Matson, Merv

RightsMarket Inc.

Matson Merv. 2002. A Policy Engine for Granting Access to Persistently Secure EHRs. Calgary, AB: RightsMarket Inc. Presented at the eHealth 2002 Conference in April 2002.
http://hdl.handle.net/1880/43131
Presentation

HEALTH 2002

Presenter Names: Merv Matson,
RightsMarket Inc

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

Track: Health Information Protection: Privacy and Security

Canadian Institute for Health Information
Institut canadien d'information sur la santé

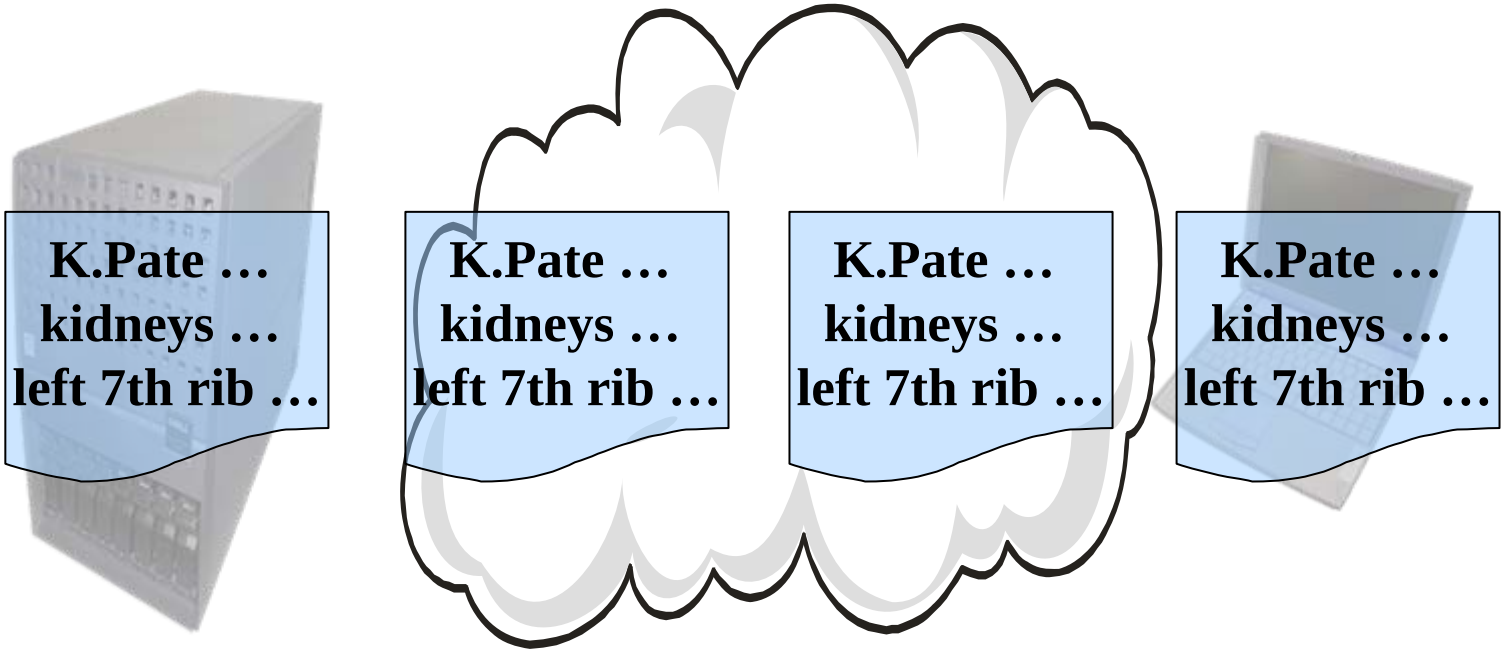
COACH
Canada's Health Informatics Association

RightsMarket

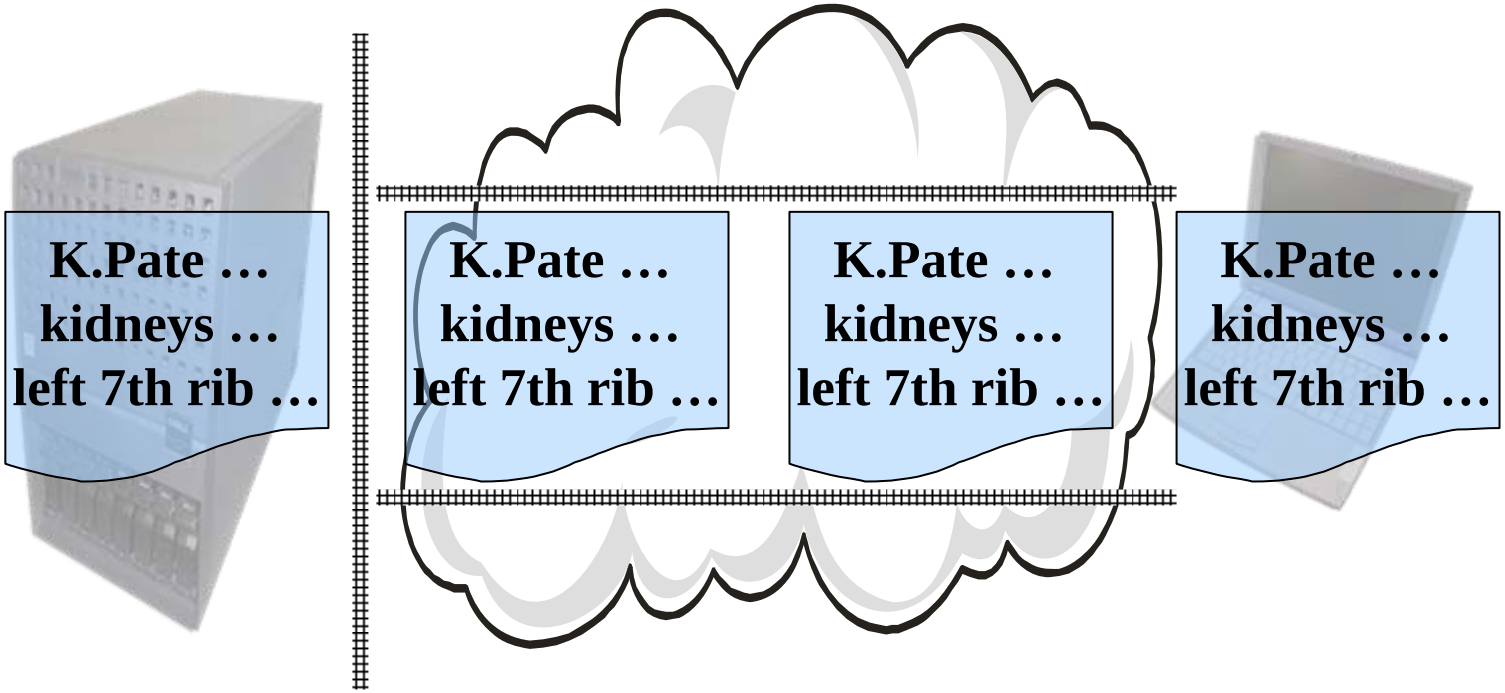
Outline A policy engine for granting access to persistently secure EHRs

- **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



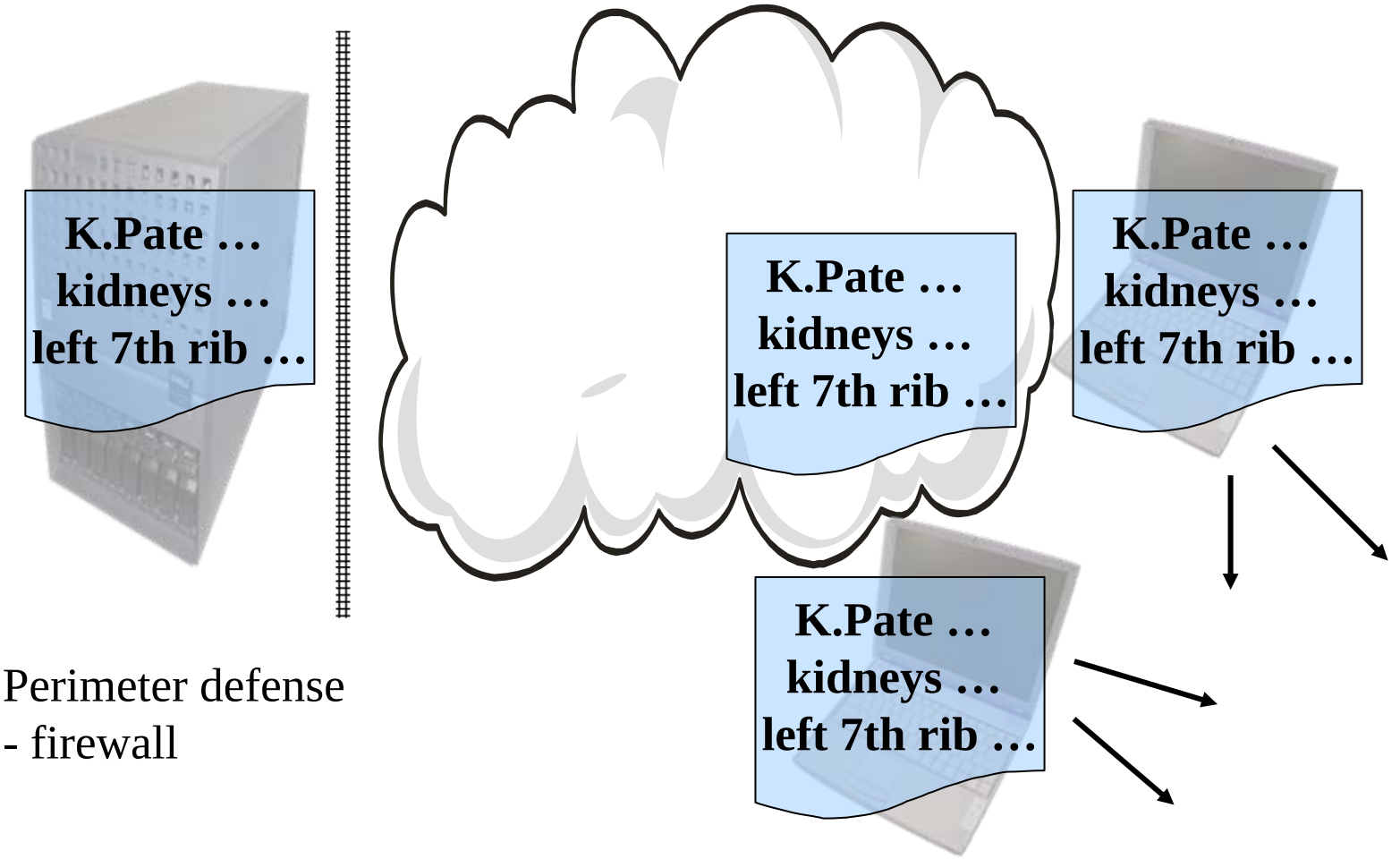
EHR Use - defenses



Perimeter defense
- firewall

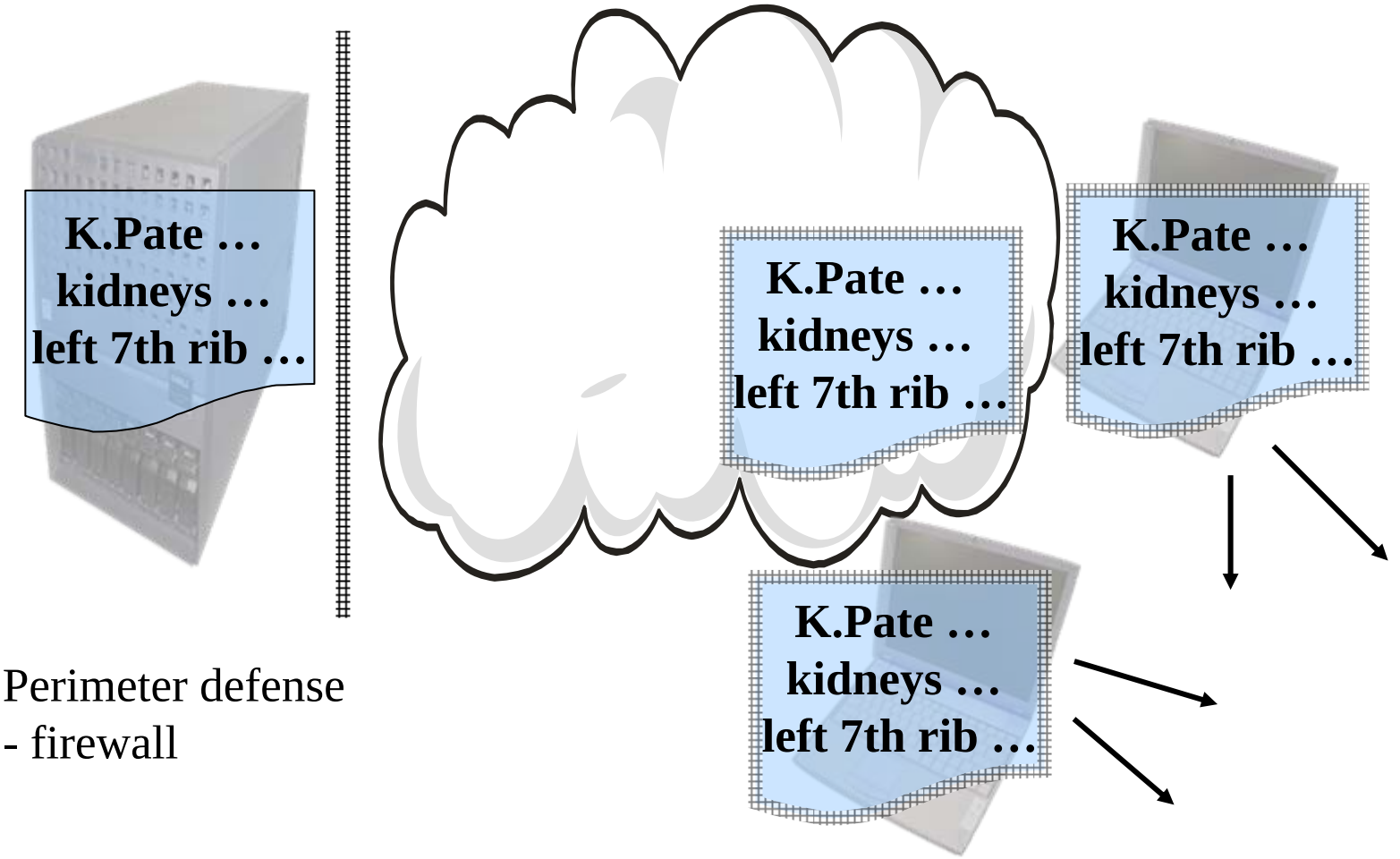
Network defense
- tunnel

EHR Use - defenseless outside



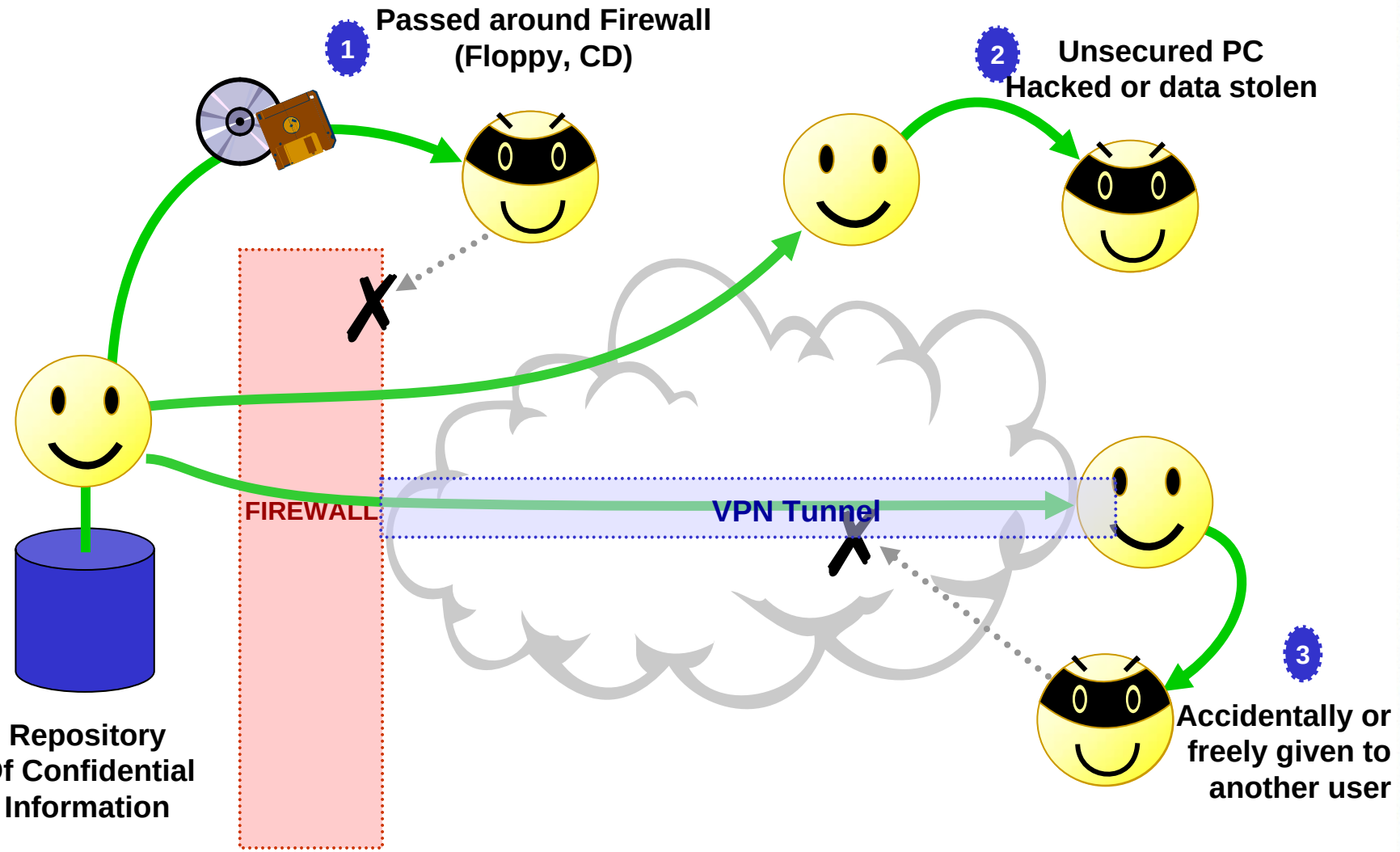
Perimeter defense
- firewall

EHR Use - protected everywhere

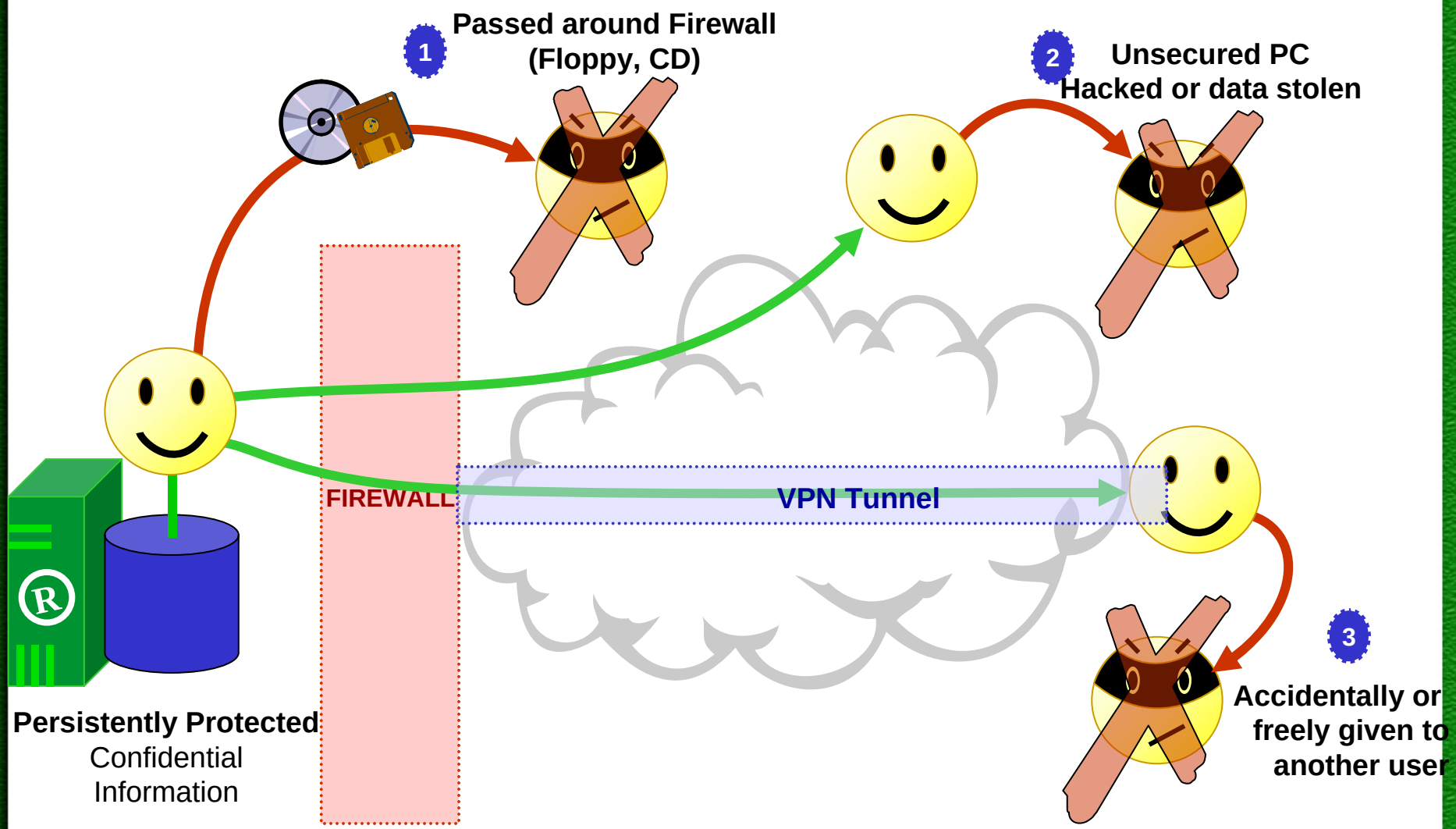


Perimeter defense
- firewall

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

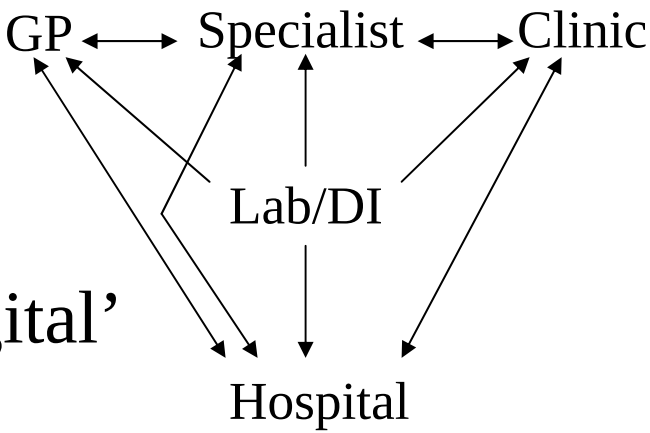
K.Pate …
kidneys …
left 7th rib …

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

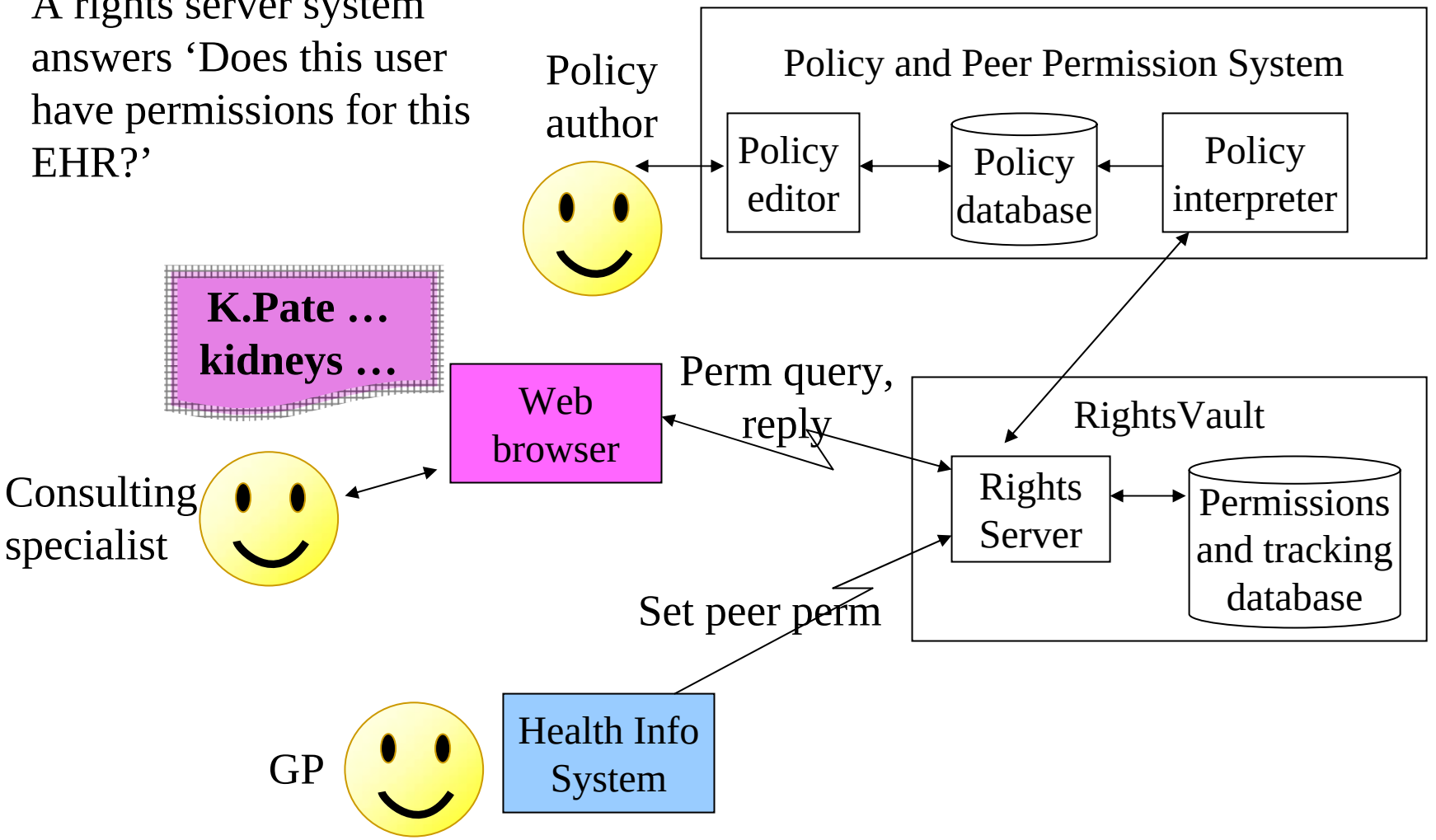
- How does the legitimate user get permission in this many to many to many relationship?
  - Many patients, each with many EMRs
  - Many potential legitimate care givers
- Coarse permissions policy? If you can get at any EMR in the repository you can get at all.
- Fine, one to one, explicit assignment?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

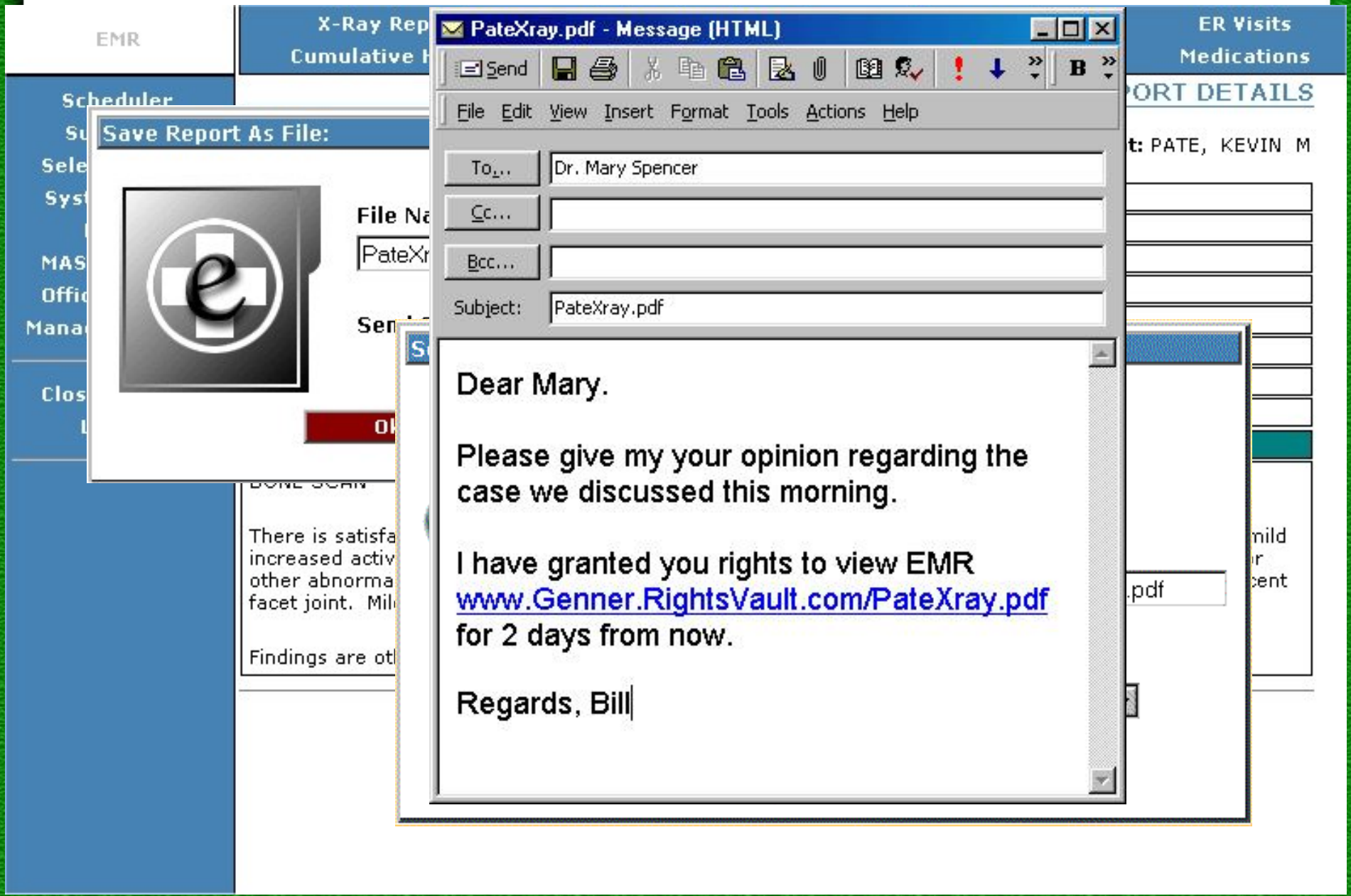
Outline A policy engine for granting access to persistently secure EHRs

- 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?’



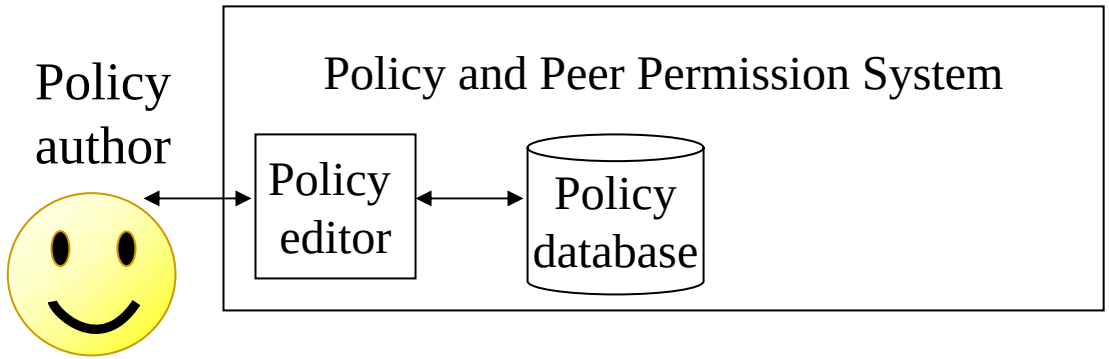


Policy Statement Examples:

- 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?

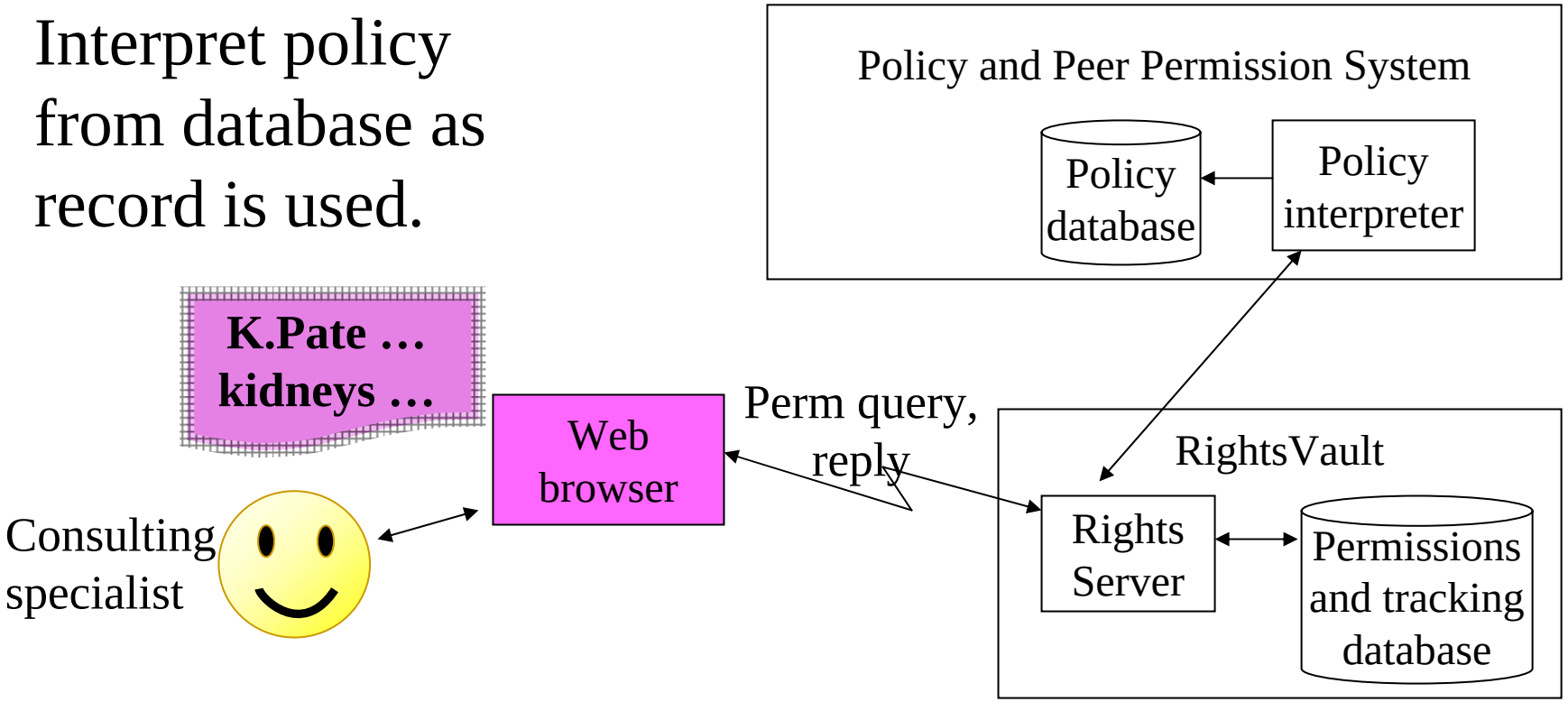
Write policy in user-friendly language, translate to machine interpretable, store in policy database



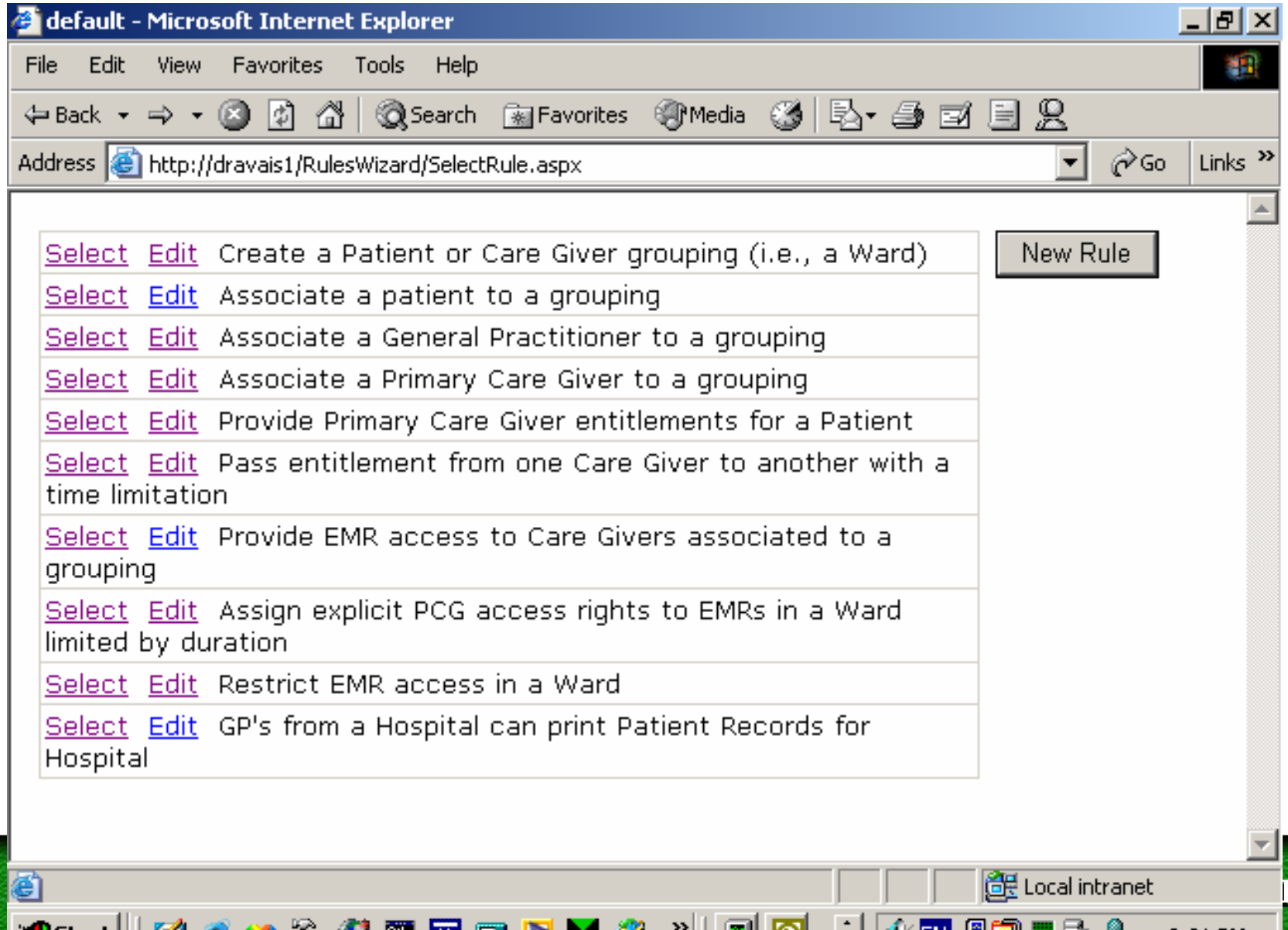
The consulting specialist assigned to me at Consulting Hospital may read all of my medical records needed for my consultation

How is it done?

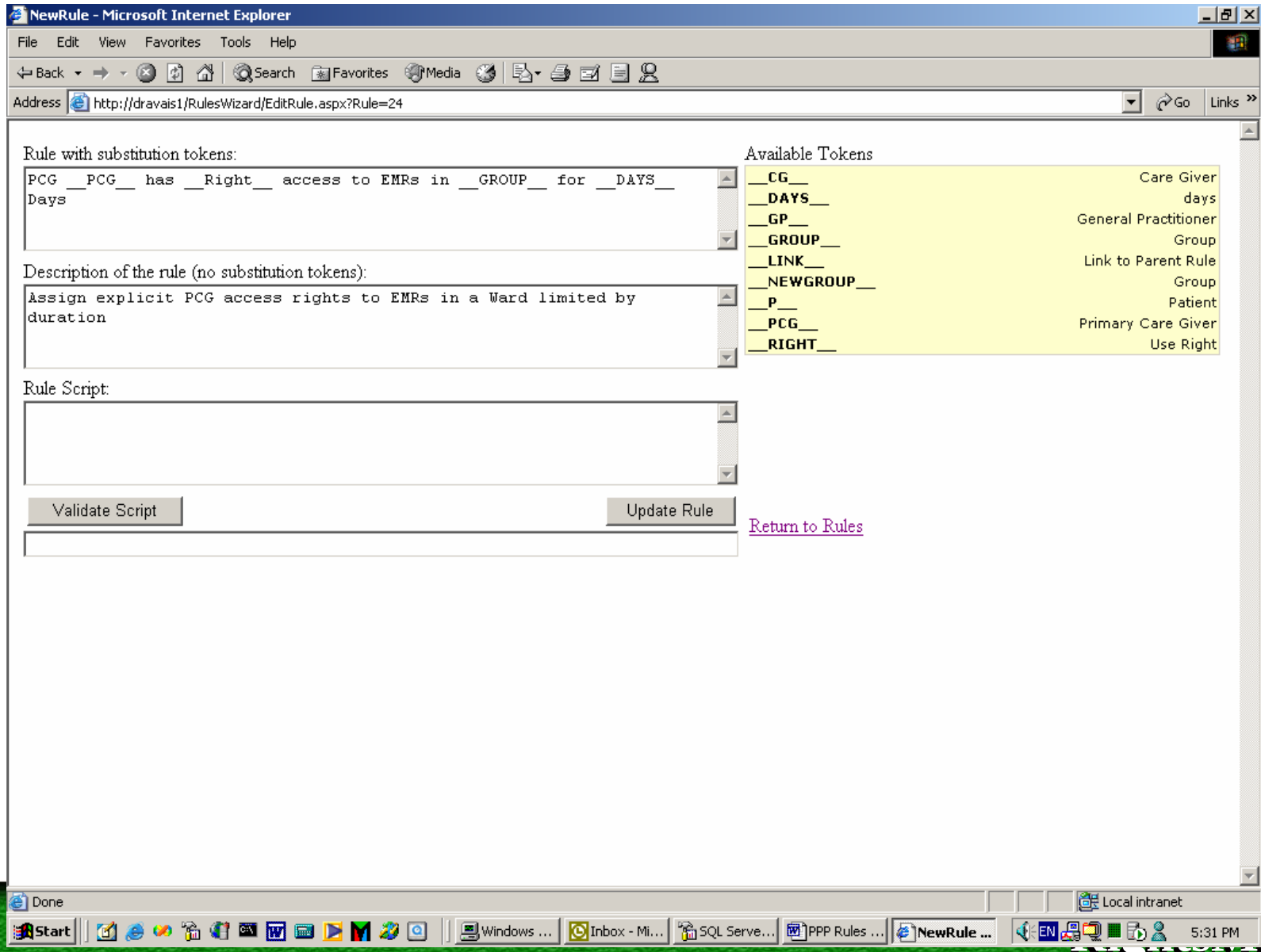
Interpret policy from database as record is used.



Write a policy: select, edit, new



Write policy: edit



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

Participant	Role	Principal Investigators
UCalgary Telehealth www.ucalgary.ca/telehealth	Policy researcher	Dr. Maryann Yeo Dr. Penny Jennett
UOttawa Heart Institute www.ottawaheart.ca	Alpha test site	Dr. Shu-Tim Cheung
RightsMarket Inc www.RightsMarket.com	Software developer	Merv Matson
CANARIE www.canarie.ca	Funder	Wendy Zatylny

How do we get to ‘sharable’?

Leave custody of records with current custodians as they go electronic

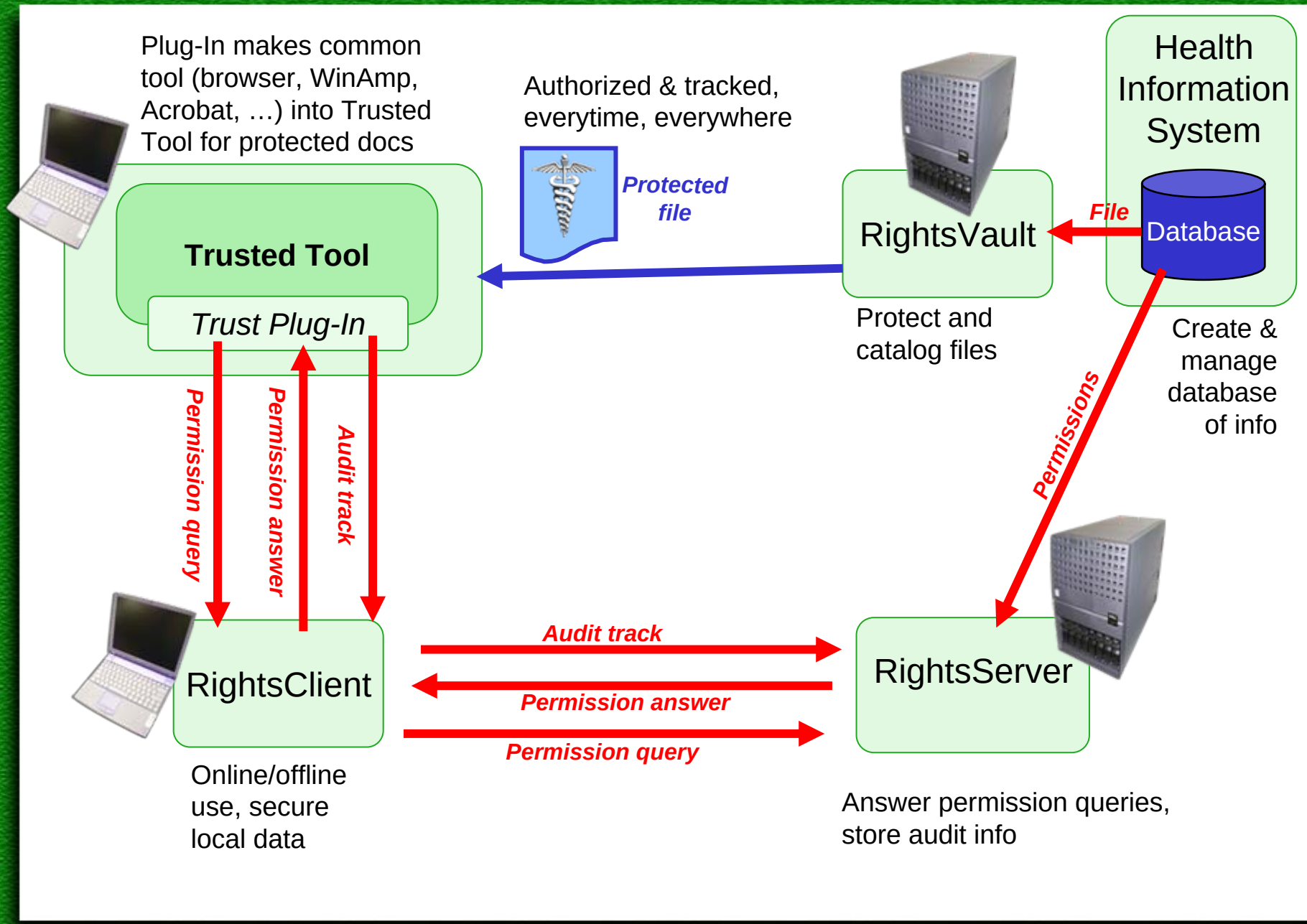
- Go **persistent**: answer the need for security at the point of use of the records, wherever that is
- Let custodians control use of persistently secured records with **policy and peer permissions**
- Make it easy for individual care givers to get started with **minimal infrastructure and buyin**; 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 tracks progress of project

Questions ?

Supplemental slides for anticipated questions



RightsMarket


ward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Real.com Messenger
www.rightsmarket.com
Best of the Web Channel Guide Customize Links Free HotMail Internet Start Microsoft Windows Update Windows
ome
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
Ideas
Quirks & Quarks
The House
As It Happens
News
ghtsMarket P
e And Q1 Fi
Repricing
tsMarket Re
sion 2.0 For Online Publishing And Music
Quick Links
RightsPublish Brochure, 328K
Get Acrobat Reader
WINAMP music player FREE
RightsMarket
digital rights management.
services to securely distribute digital content and prevent
ry. Offering solutions for both text and audio in the areas of
h, RightsMarket enables organizations to capitalize on the
distribution over the Net.
ts management, RightsMarket offers Systems Integration (SI) services that
larket technology to provide custom solutions tailored to our clients' needs.
d services to
manage
and
istribute
gital content.
The company's flagship product, RightsPublish, is an end-to-
solution for selling, securing and tracking digital content. Eas
implement, RightsPublish provides a Web storefront,
eCommerce, complete audit trail, and persistent security. Se
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.

Genner's PC

- EMR: PateXray

1a. Protect, catalog, generate installers, set permission

RightsVault

- EMR: PaulHistory
- EMR: PateXray

2. Ask opinion

3. Download

1b. Set useright

RightsServer

- File: Userights
- Genner, PaulHistory, 1 yr.
- Spencer, PateXray, 2 days

Spencer's Laptop

- EMR: PateXray
- Trusted Tool
- RightsClient

UseRight:

- PateXray, 2 days

4b. Useright? (PateXray)

4c. Useright (PateXray,2 days)

Open PateXray offline

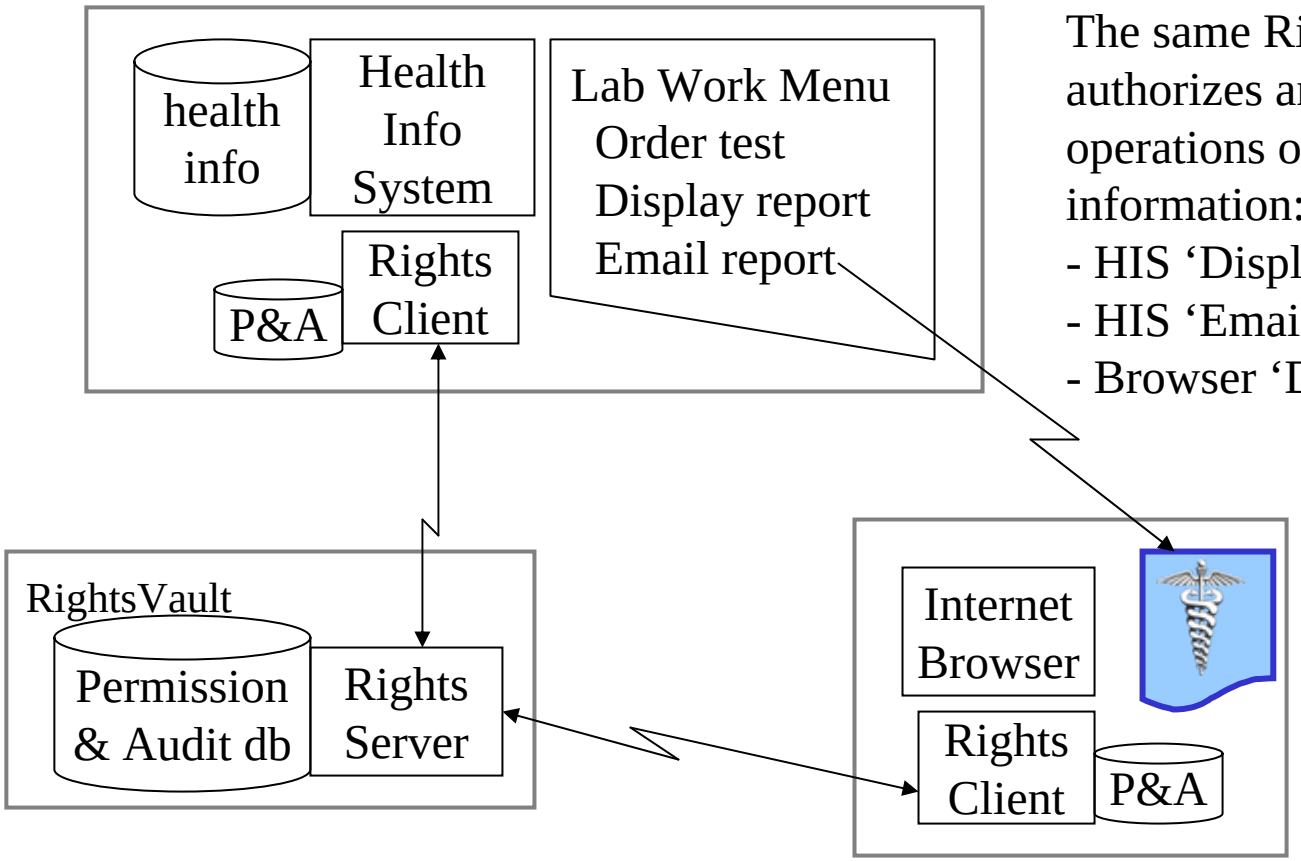
PateXray

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 Genner	2001-11-08 13:07	132457; read, 2 day from set
PateXray	open	132457 Spencer	2001-11-08 15:33	close 2001-11-08 15:36
PateXray	open	132457 Spencer	2001-11-08 19:13	close 2001-11-08 19:26

Integrated Authorization and Tracking



The same RightsVault system authorizes and tracks all three operations on the same information:

- HIS ‘Display report’
- HIS ‘Email report’
- Browser ‘Display report’.

Conclusion

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

For more information

www.RightsMarket.com > Solutions > RightsVault
> Solutions > Customers > CBC
> Demo

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

Security – Risk Model

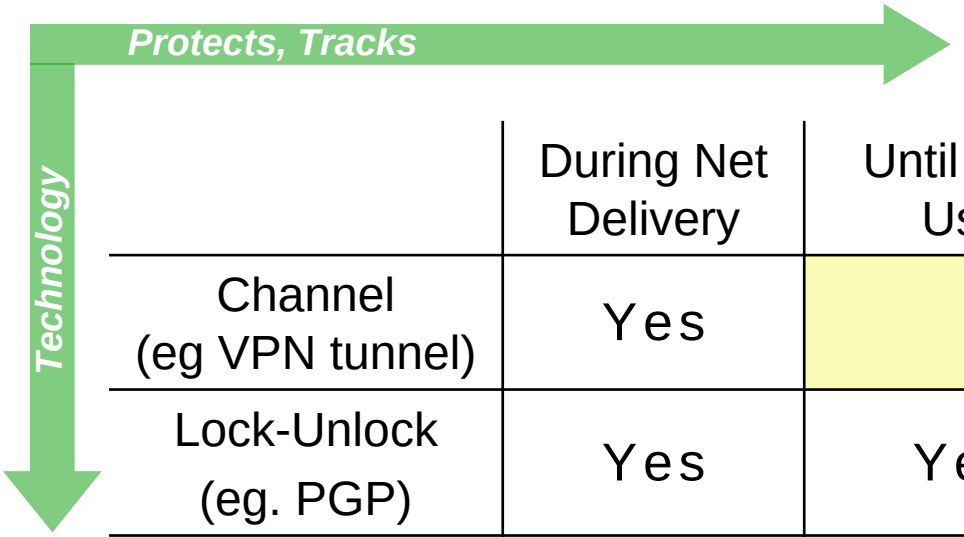
Security Strength

Location	Attack, Risk	VPN	Persistent
Authentication	Impersonation; false qualification	Strong[1,2]	Light[3,4]
At Host System	Hack attack; carelessness; mischief	NA[5]	NA/Strong[6]
In Net Transit	Intercept, crack encryption	Strong	Strong
At Point of Use	Hack attack; carelessness; mischief	NA[5]	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 (eg VPN tunnel)	Yes		
Lock-Unlock (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