Enabling Robust Information Accountability in E-healthcare Systems

USENIX HealthSec '12
Bellevue, WA
8/7/2012

Daisuke Mashima
Mustaque Ahamad

College of Computing
Georgia Institute of Technology
Atlanta, GA, USA

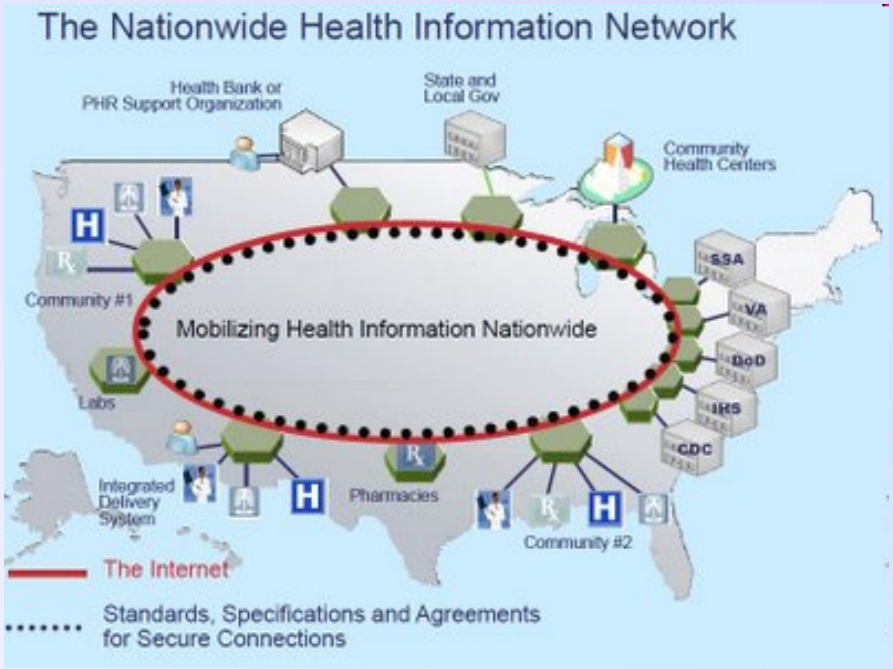
Outline

- Background / Motivation
- User-centric Monitoring Agent System
- Enabling Actionable Accountability
- Prototype Implementation & Performance
- Conclusions

Background

- Transition from paper-based records to electronic health (medical) record
  - Electronic Health Record (EHR) systems
  - Personal Health Record (PHR) systems
- “Meaningful Use” incentive program by CMS
  - HITECH Act in 2009
- Initiatives for large-scale health information exchange
  - Nationwide Health Information Network (NHIN)
  - NHIN Direct

Microsoft® HealthVault™



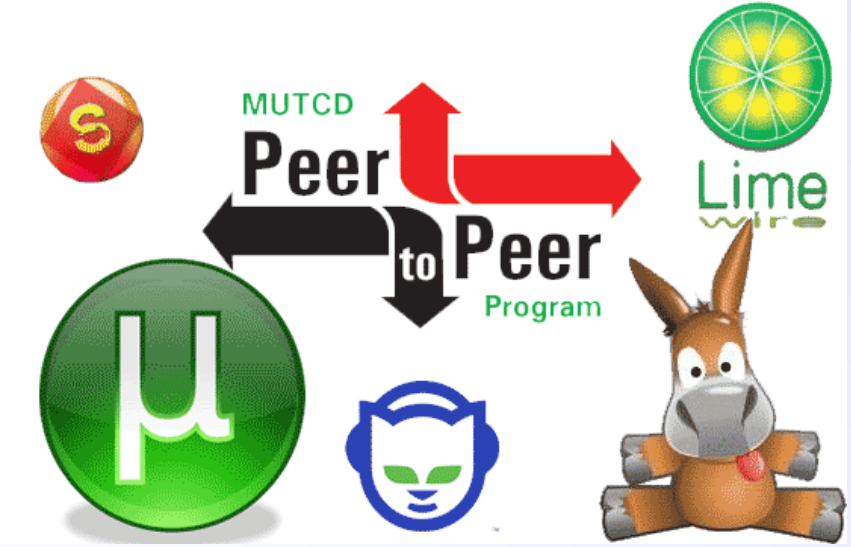
Misuse of Health Information

*In September, 2006, **one front desk office coordinator** at Cleveland Clinic in Weston, FL was indicted for committing healthcare fraud. She abused her access privilege to download healthcare records of more than 1,100 patients. She then sold them to **her cousin**, who owned a medical claims company in Florida and filed false claims to **Medicare** to gain approximately $2.8 million*.

Data Breach by Insiders

- *According to HHS, a large number of data breach cases are caused through lost or stolen devices used in healthcare organizations.*

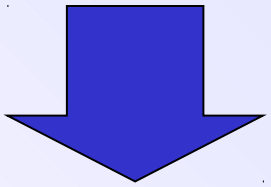
- *Yet another possibility…*



Accountability for EHR Sharing / Usage

- Assurance of knowledge about how an EHR reaches a certain health record consumer

- Providing patients with verifiable evidence about who is involved in the sharing path of a certain EHR



Provide patients with awareness and actionable information
Discourage malicious / inappropriate handling by insiders

Related Work

- Information accountability
  - Weitzner et al. (2008)
    - “The use of information should be transparent so it is possible to determine whether a particular use is appropriate … and that the system enables individuals and institutions to be held accountable for misuse.”
    - Visibility, under established rules, can encourage compliance.
- Auditing in healthcare organizations
  - King et al. (2012)
    - Current EHR systems have major weakness with “user-based non-repudiation”.
    - Possibility of tampering or forgery by a system administrator
- Data provenance
  - Aldeco-Perez et al. (2008), Kifor et al. (2008) etc.
  - Derivation history of each data
  - Created based on a set of assertions.
  - Centralized assertion store is not often realistic.

User-centric Monitoring Agent for Enhancing Users' Awareness

(ACM IHI 2012)

User-centric Monitoring Agent

- User-controlled “reference monitor” to mediate accesses to data in a distributed setting
  - Reliable mediation under assumptions reasonable in recent e-healthcare settings
- An online service deployed on an entity trusted (chosen or managed) by each patient

Scope and Assumptions

- Allows patients to be aware of by whom and when their health records are meaningfully consumed.
  - Meaningful usage of health records is accompanied by integrity/authenticity verification.
    - Legitimate consumers (Medicare etc.) are naturally motivated to do so.
    - Adversaries can obtain meaningful gain only by presenting health data to legitimate consumers.
  - HIPAA Section 164.520 "Notice of privacy practices"
- A repository accepts new records (or update of record) only under patient's awareness.
  - Justified by patient's right noted in Section 164.524 of HITECH Act.
- PKI is established and every participant is assigned a key pair by one of trust anchors.
  - Under NHIN Direct standards, PKI is required.

Architecture Overview

Monitoring Agent

Hospital A

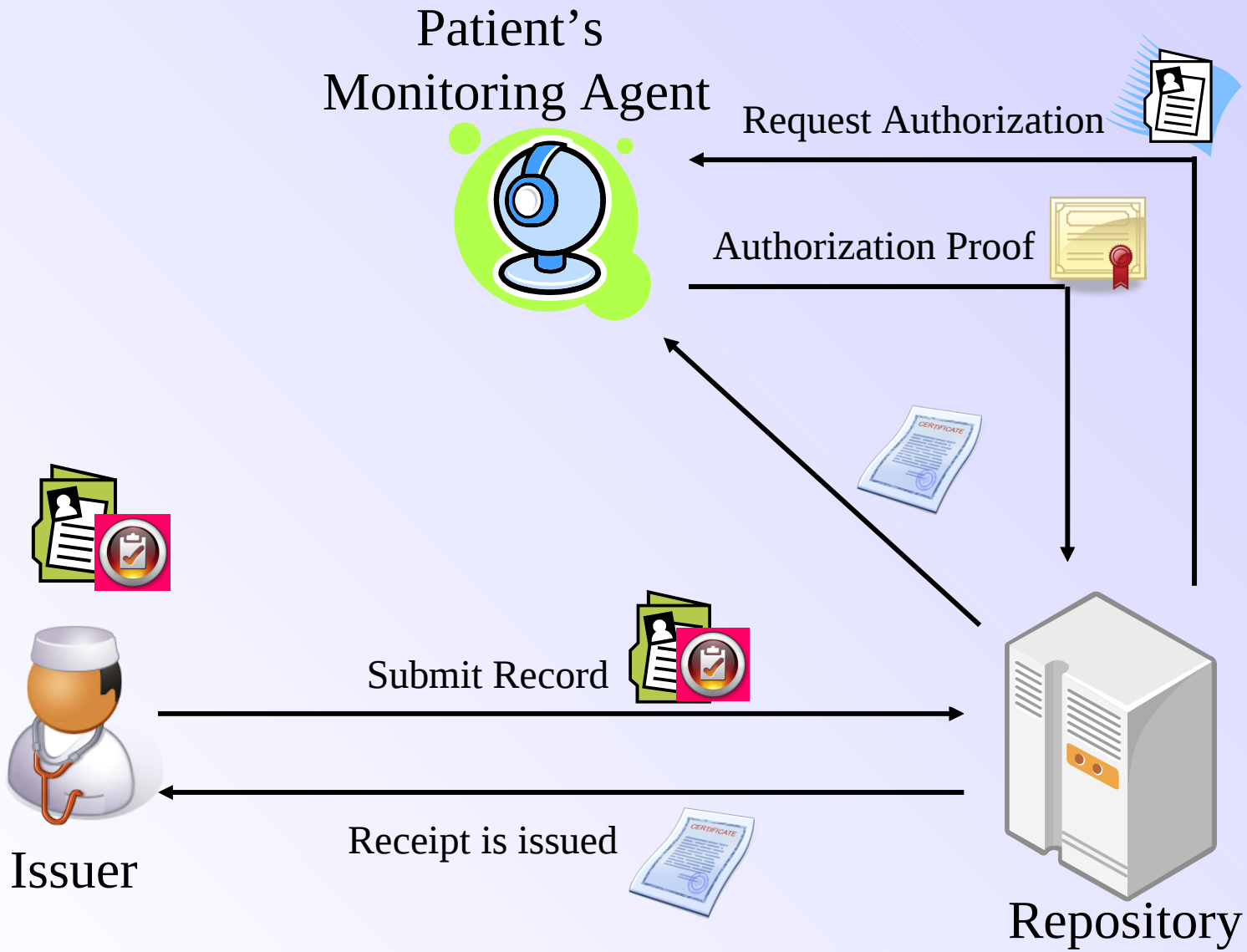
Doctor (Issuer)

Repository

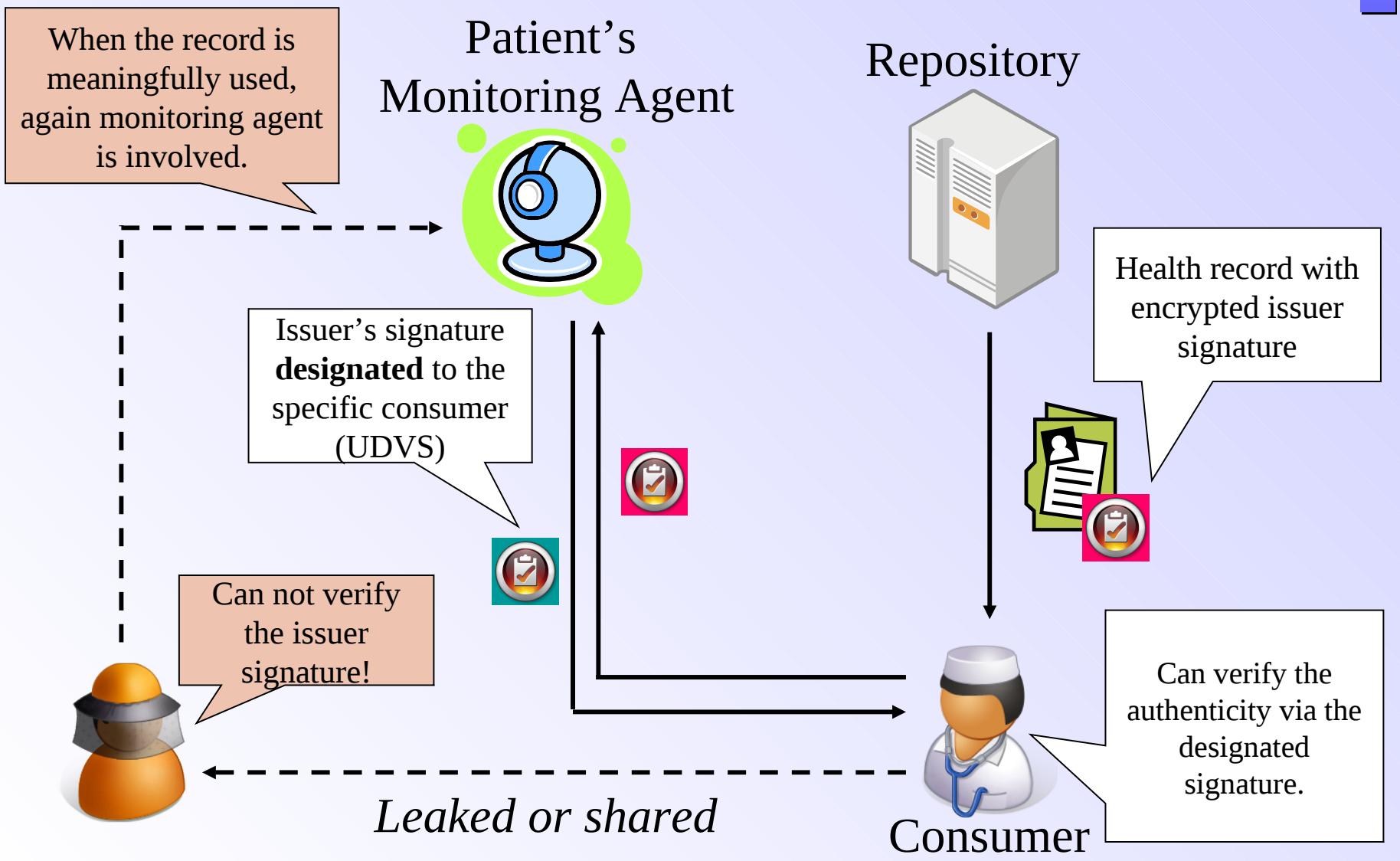
Hospital B

Doctor (Consumer)

Update of Health Record
(Accountable Update)



Usage of Health Record *(Accountable Usage)*



Enabling Actionable Accountability

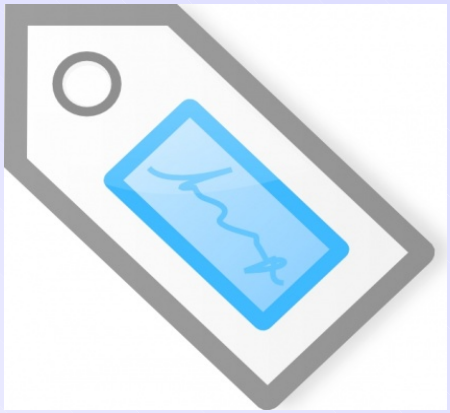
Identifying The Source of Breach

- Awareness alone is not sufficient.
  - In case of misuse, it is often not possible to determine the responsible entities.
- Lack of actionable accountability would encourage insider threats.

Accountability Tag

- Metadata that is attached to each copy of healthcare records.
  - Conveys information about the one-hop EHR sharing.
  - Accumulated tags enable a patient to re-construct the complete sharing path.

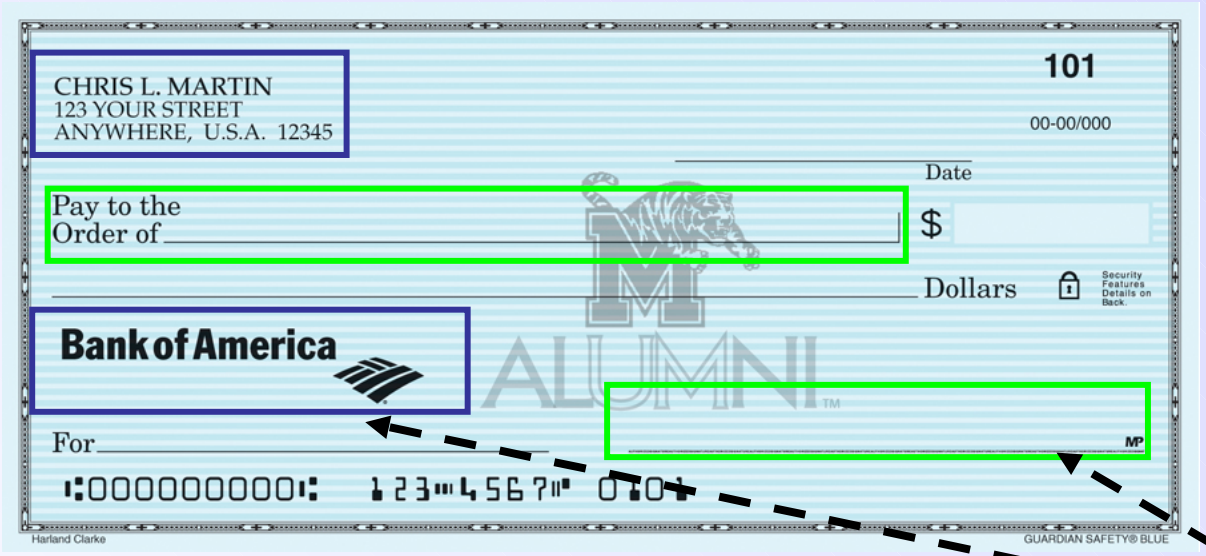
- Verified and logged by a patient's monitoring agent when:
  - *Accountable Usage* is run.
  - A shared record is submitted via *Accountable Update.*

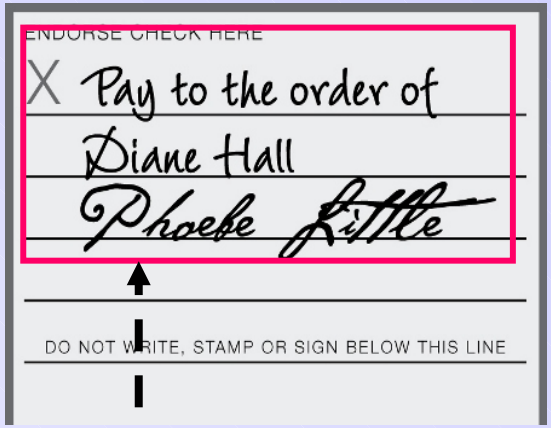


Accountability Tag

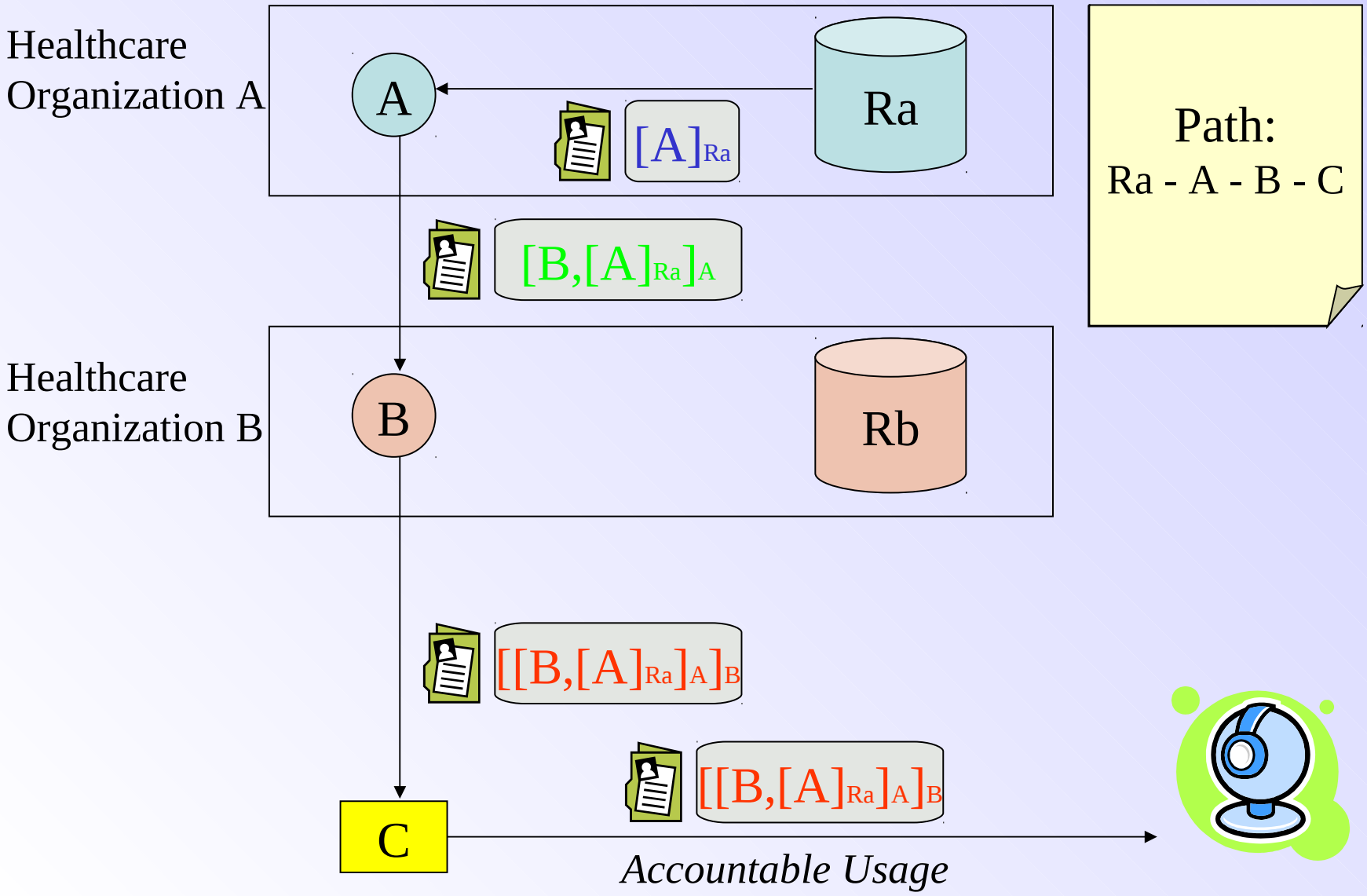
- 3 stages of accountability tags:
  - PreTag
    - Issued (signed) by **a repository** that releases a healthcare record and signed along with the downloader's (A's) identity.
  - Tag (Activated)
    - Signed by **a source of healthcare record sharing** (A) with the recipient's (B's) identity.
  - CTag (Confirmed)
    - Signed with **the designated recipient**'s (B's) private key.

Analogy to Personal Check

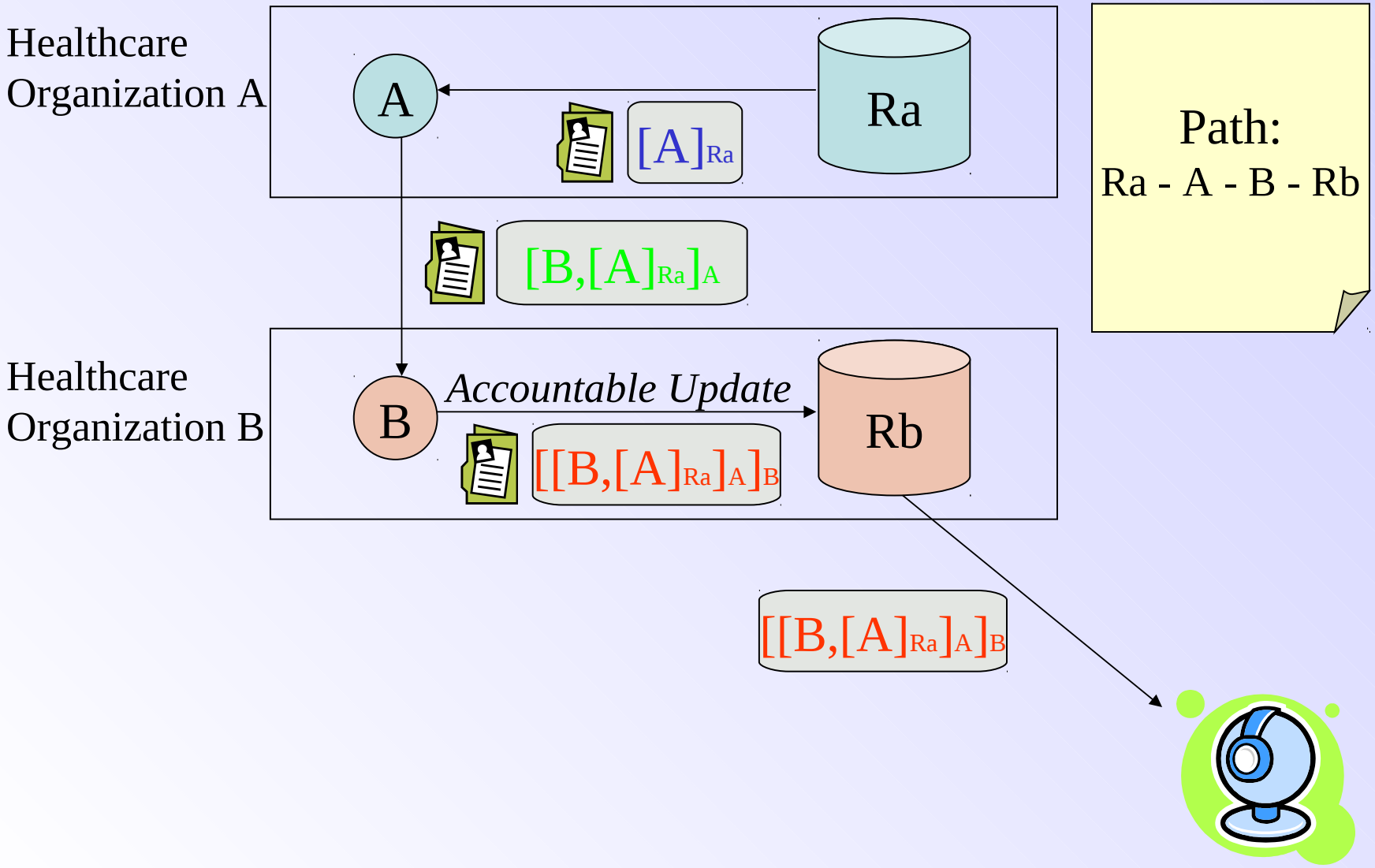




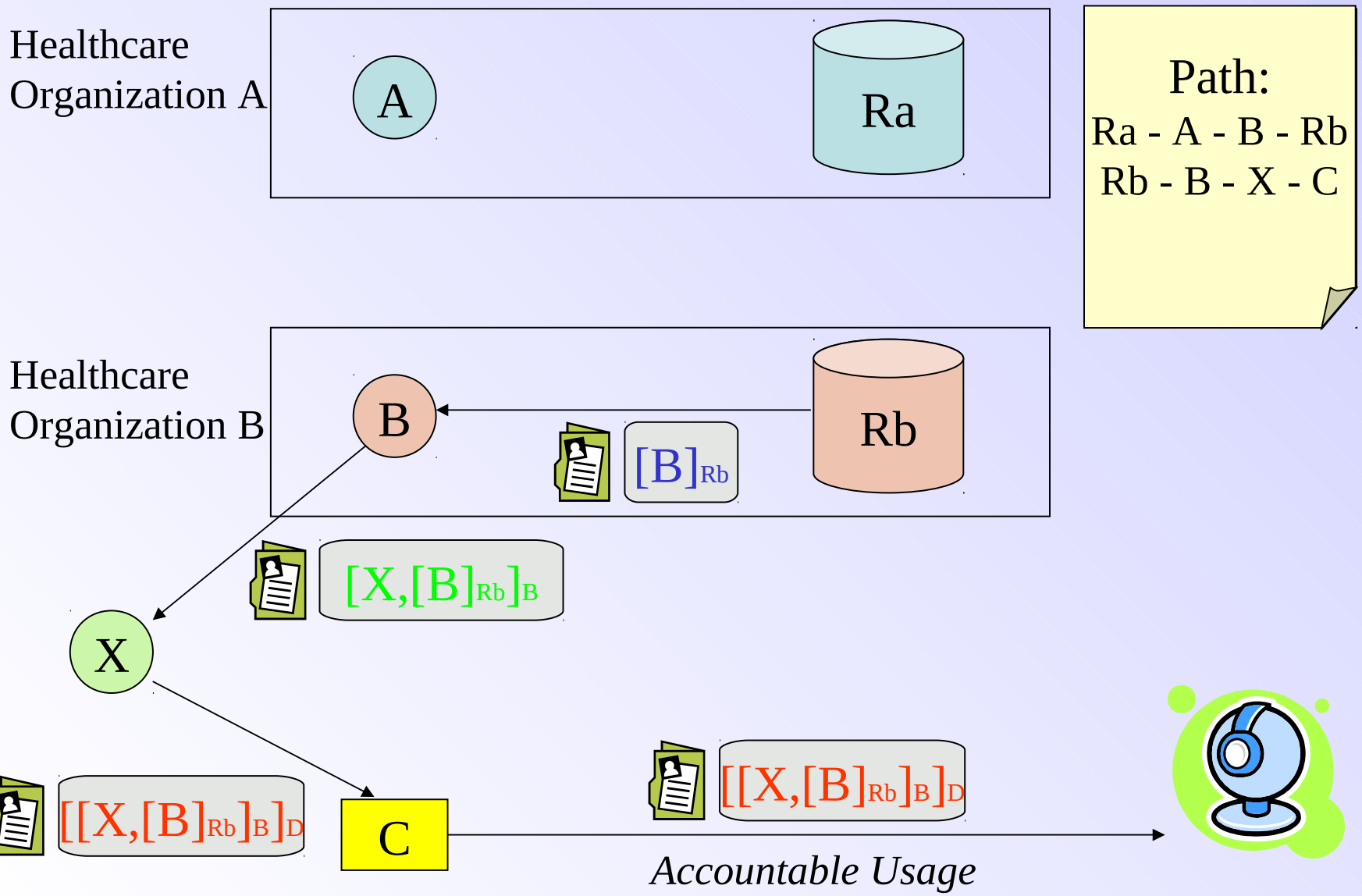
Accountability Tag System



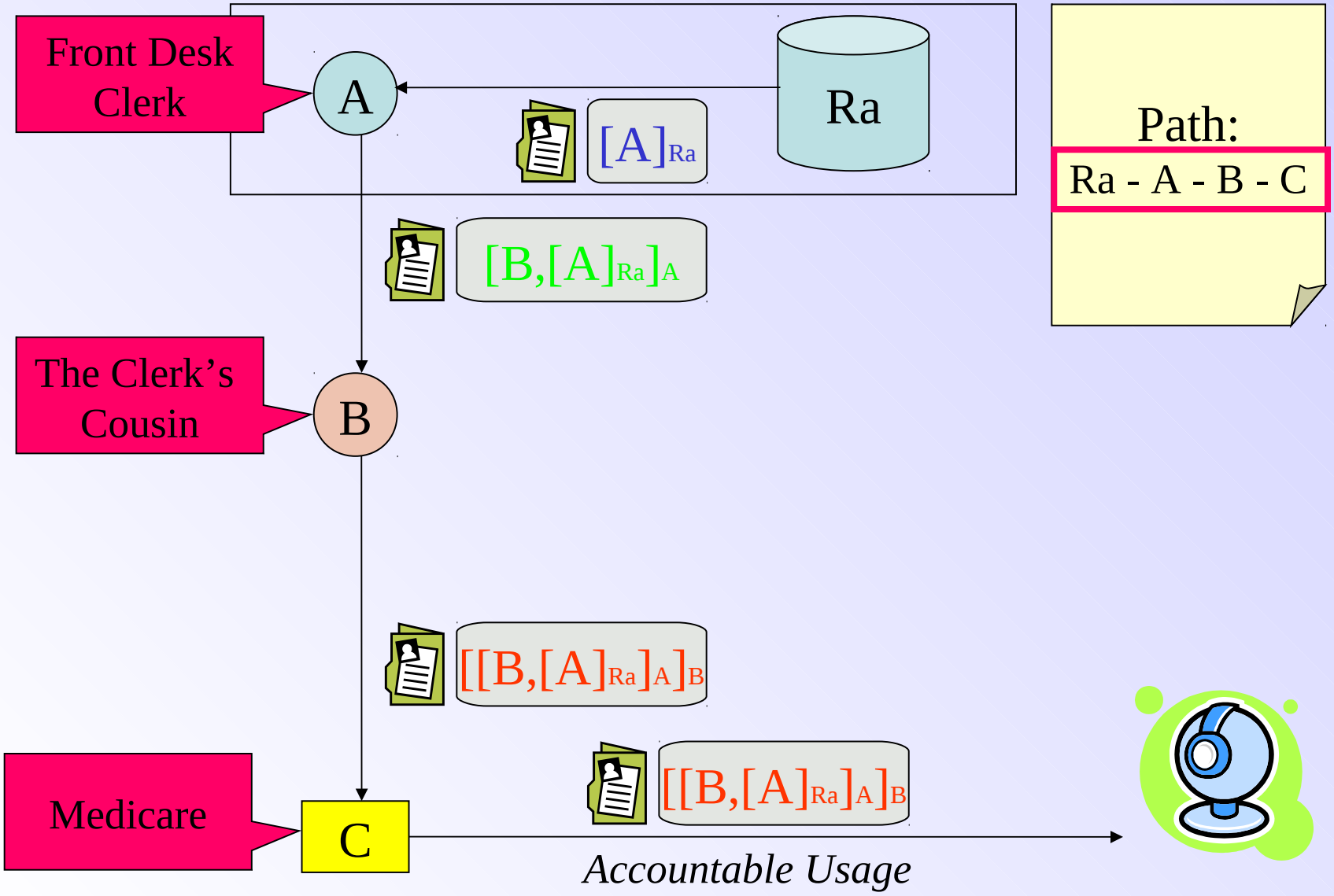
Accountability Tag System



Accountability Tag System

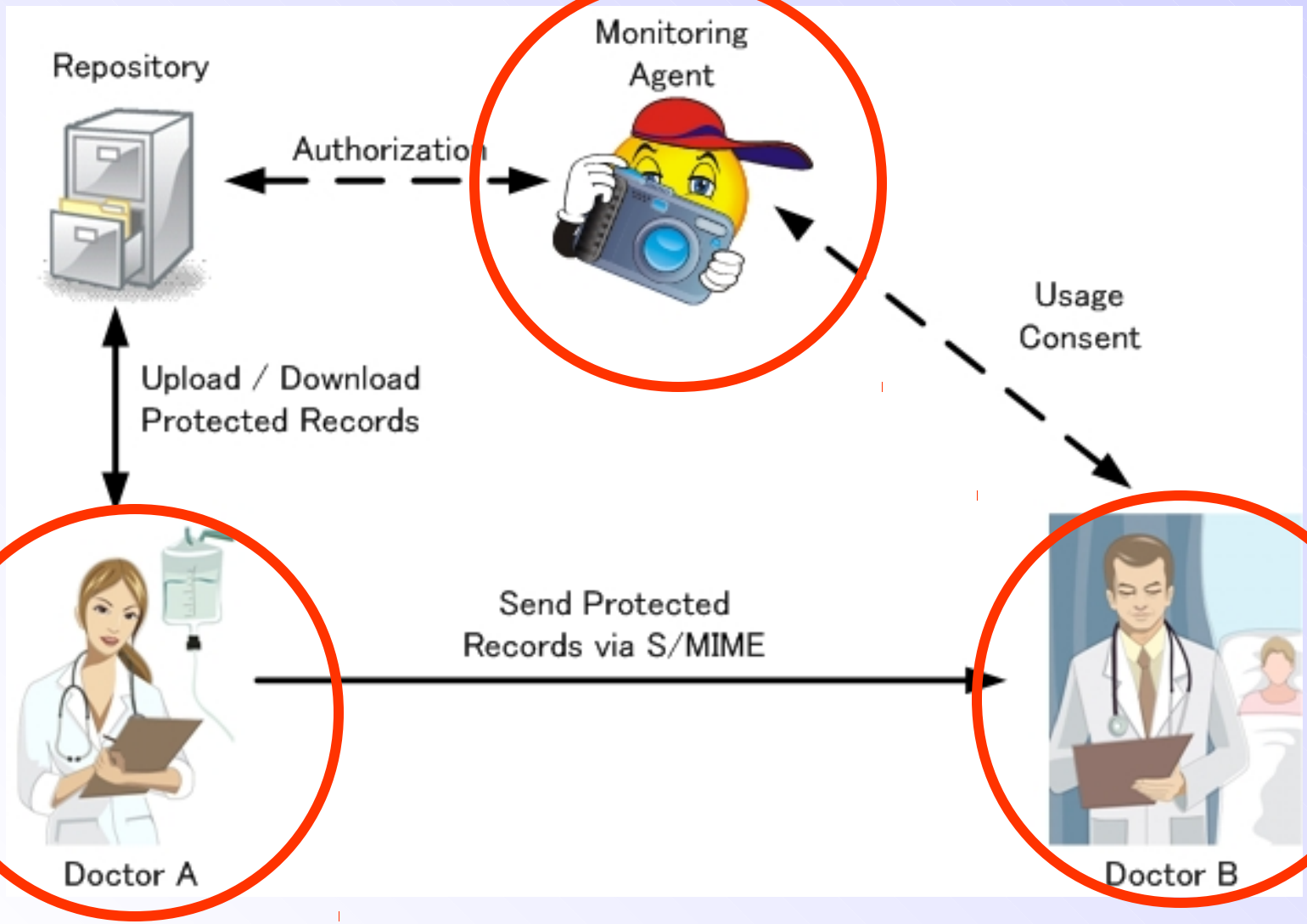


Case Study: Cleveland Clinic Case



Prototype Implementation

Integration in NHIN Direct



Overhead for Robust Accountability

Task	Response Time w/o Acct. Tag [ms]	Response Time w/ Acct. Tag [ms]
Tag Activation	0	15.47 (4.08)
Tag Confirmation	0	15.18 (4.29)
Acct. Usage (3MB)	1,151.33 (113.99)	1,345.83 (106.3)
Acct. Usage (6MB)	1,792.65 (41.58)	1,560.31 (149.28)
Acct. Update (3MB)	4,957.17 (227.27)	4,530.44 (82.35)
Acct. Update (6MB)	9834.60 (62.62)	9,117.53 (123.28)

Overhead for additional accountability guarantee is far less than 1 second.

Conclusions

- Assurance of information accountability
  - A patient can know how the record reached consumers from the source repository.
  - A patient can know which organization stores copies of her records.
- Mitigation of risks owing to lost / stolen health records
  - Absence of an accountability tag does not allow healthcare records to be meaningfully consumed.
- Patient's control over EHR usage / update
  - Implemented through a "black list" on a patient's monitoring agent.

Thank you very much.

mashima@cc.gatech.edu
http://www.cc.gatech.edu/~mashima