HIPAA as Workflow

Roy Rada, M.D., Ph.D.
Prof. Information Systems
UMBC

HIPAA@IT:
Health Information
Transactions,
Privacy, and Standards
www.hypermediasol.com

1 Executive Summary

- Viewed as workflow management, HIPAA can be re-interpreted as fundamental to improving efficiency.
- Transactions standards are for communicating.
- 'Minimum necessary use' is the heart of privacy and essentially a workflow matter.
- The best way to achieve security is to have appropriate workflow.
- Cases, such as Kaiser, support this view.

Audience participation required!!

2 Table of Contents

3 What is workflow?

Not in Merriam-Webster’s Collegiate Dictionary but

webopedia (webopedia.internet.com) says: Workflow is a defined series of tasks within an organization to produce an outcome.

Workflow management systems support the management of workflow.

Workflow Management Coalition (www.wfmc.org) emphasizes a hierarchical decomposition from processes to sub-processes to activities to work items that are then executed either by people or by machines.

Center for New Engineer defined:

Image-based workflow systems transfer traditional media like health insurance claims to digital 'images' and then route them based on text-fields associated with the images.

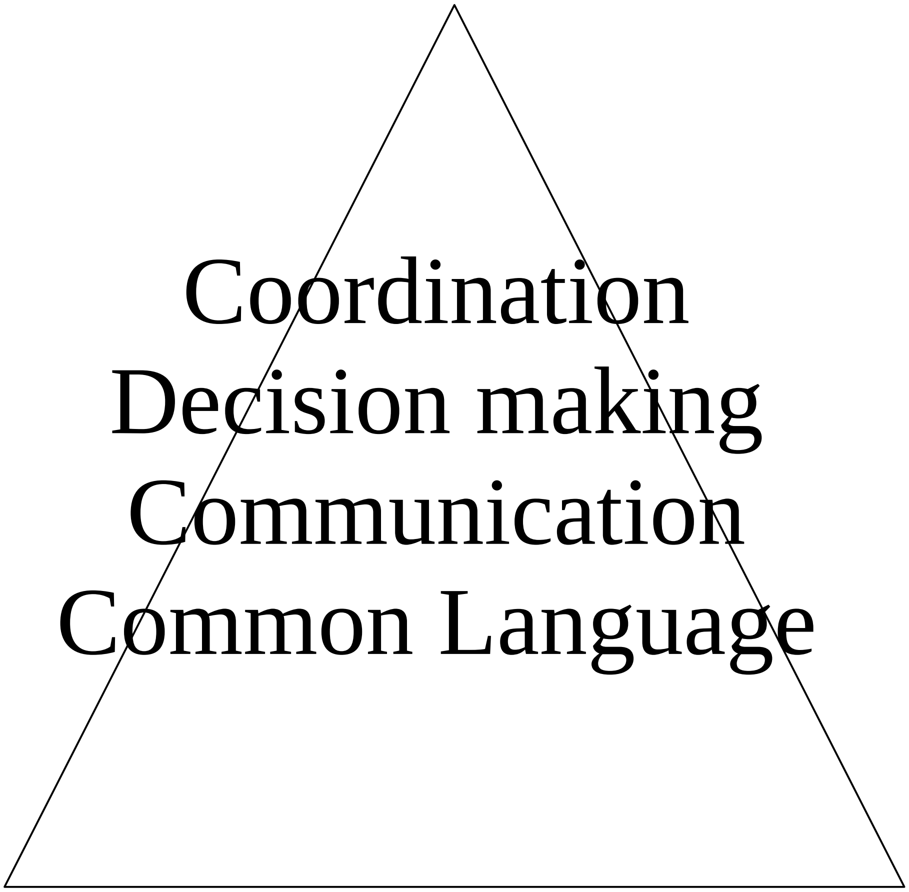
Form-based workflow systems may semi-automatically update the fields on a schedule.

These become coordination-based workflow systems that focus on the entire organization achieving its mission.

Workflow management includes

- information flow management and
- knowledge management

4 Coordination



Coordination
Decision making
Communication
Common Language

MIT Center for Coordination Science (http://ccs.mit.edu)

4.1 Common language

- code sets. for instance:
  - ICD-9-CM for diagnosis,
  - CPT-4 for procedures, and
  - race categories for race

- transaction envelopes. for instance:
  - interchange control header,
  - functional group header,
  - transaction set header,
  - data segment,
  - data element

4.2 Communication

- patterns of X12 messages. For example:
  - provider sends 270 eligibility inquiry to payer for enrollment and
  - payer sends 271 eligibility information to provider.

- privacy notice

4.3 Decision-making

- certain diagnoses correspond to certain reimbursements (first A in HIPAA is for "Accountability" and getting right reimbursement for patient condition).
- minimum necessary use of information according to role responsibility
- patient can request to amend the record and covered entity can review and reject

4.4 Coordination

- transactions should increase efficiency
- privacy should give further power to patient

5 Privacy

5.1 Minimum Necessary Use

An entity must identify the

- classes of persons who need access to information,
- categories of information to which such persons need access, and
- conditions that apply to such access.

Roles: People are classified according to the functions they serve.

Information is also categorized.

Roles are mapped to information categories.

Entities must limit access to the identified persons, and the identified information.

For example

- a hospital could implement a policy that permitted nurses access to all protected health information of patients in their ward while they are on duty.

- a health plan could
  - permit its underwriting analysts unrestricted access to aggregate claims information for rate setting purposes, but
  - require documented approval from its department manager to obtain specific identifiable claims records.

5.2 Notice of Privacy Practice

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

....

In most cases, you have the right to look at or get a copy of health information about you that we use to make decisions about you. If you request copies, we will charge you $0.05 (5 cents) for each page. You also have the right to receive a list of instances where we have disclosed health information...

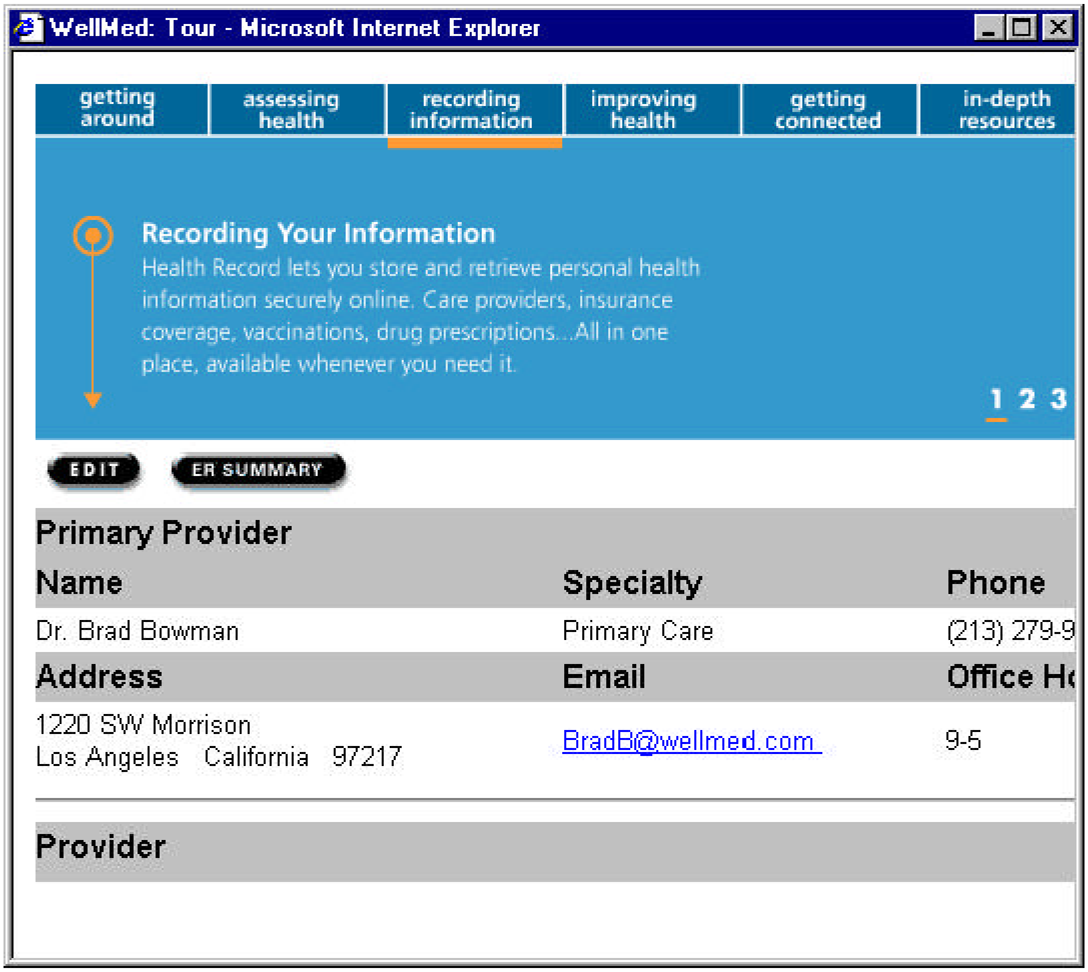
5.3 CPRI Employee Form

Each person accessing (HEALTHCARE ENTITY) data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. Therefore, all persons who are authorized to access .... must read and comply with (HEALTHCARE ENTITY) policy.

5.4 Patients

- Patients have new rights of access, amend, and account under Privacy Rule.
- These rights bring the patient into the healthcare workflow.

- www.wellmed.com illustrates patient in workflow



Recording Your Information

Health Record lets you store and retrieve personal health information securely online. Care providers, insurance coverage, vaccinations, drug prescriptions...All in one place, available whenever you need it.

Primary Provider

Name	Specialty	Phone
Dr. Brad Bowman	Primary Care	(213) 279-9
Address	**Email**	**Office H**
1220 SW Morrison Los Angeles California 97217	BradB@wellmed.com	9-5

Provider

6 Security

Security policies cover

- confidentiality: controlling who gets to read information,
- integrity: assuring that information is changed only in a specified and authorized manner, and
- availability: assuring that authorized users have continued access to information and resources.

Implemented in 3 levels

- Real-World Policy
- Computer Models
- Technical Mechanisms

6.1 Real-World Policy: Kaiser

Kaiser has User, Manager, and Trustee roles

User is responsible for

- maintaining the confidentiality of data
- complying with policy
- ..

Manager is responsible for

- reviewing job responsibilities
- requesting access for users who need it
- ….

Trustee is responsible for

- determining how a business application and its data are used
- auditing use of the application and its data
- …

Kaiser classifies data

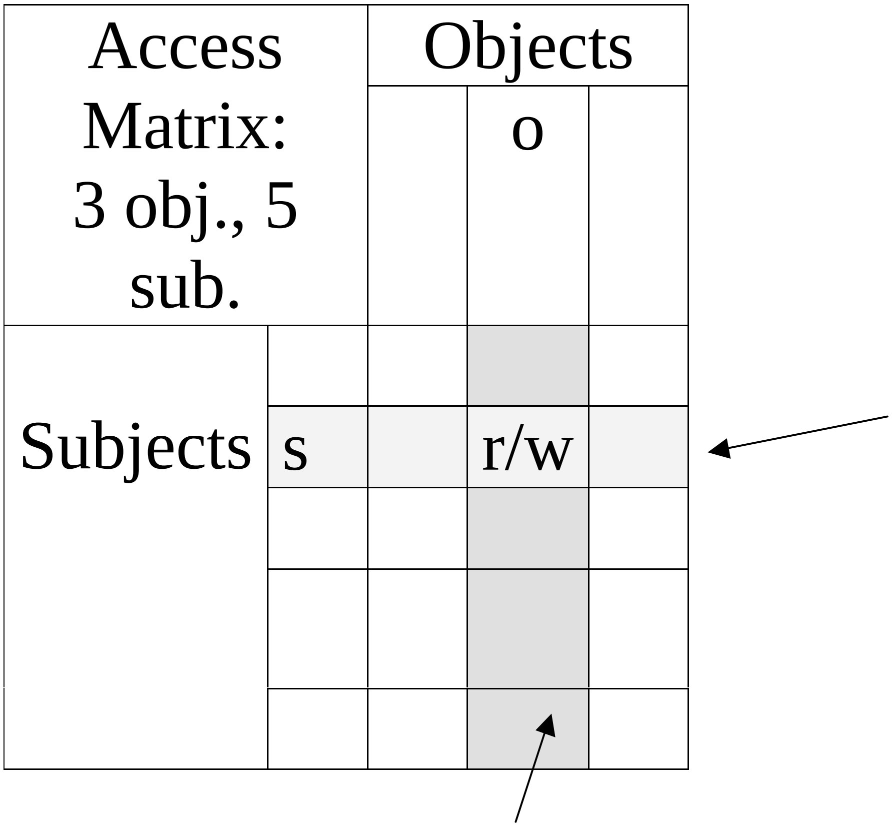
- Public: press release
- Internal: internal phone book
- Confidential: patient treatment data
- Registered confidential: mental health treatment data

Delineate many more User roles such as coronary care nurse, receptionist, radiology technician, ….

Map roles to data with what need to do when.

Manager and Trustee help administrate the User roles as regards privacy/security.

6.2 Computer Models



Access Matrix: 3 obj., 5 sub.

Objects

o

Subjects

s

r/w

capability list for s

access control list for o

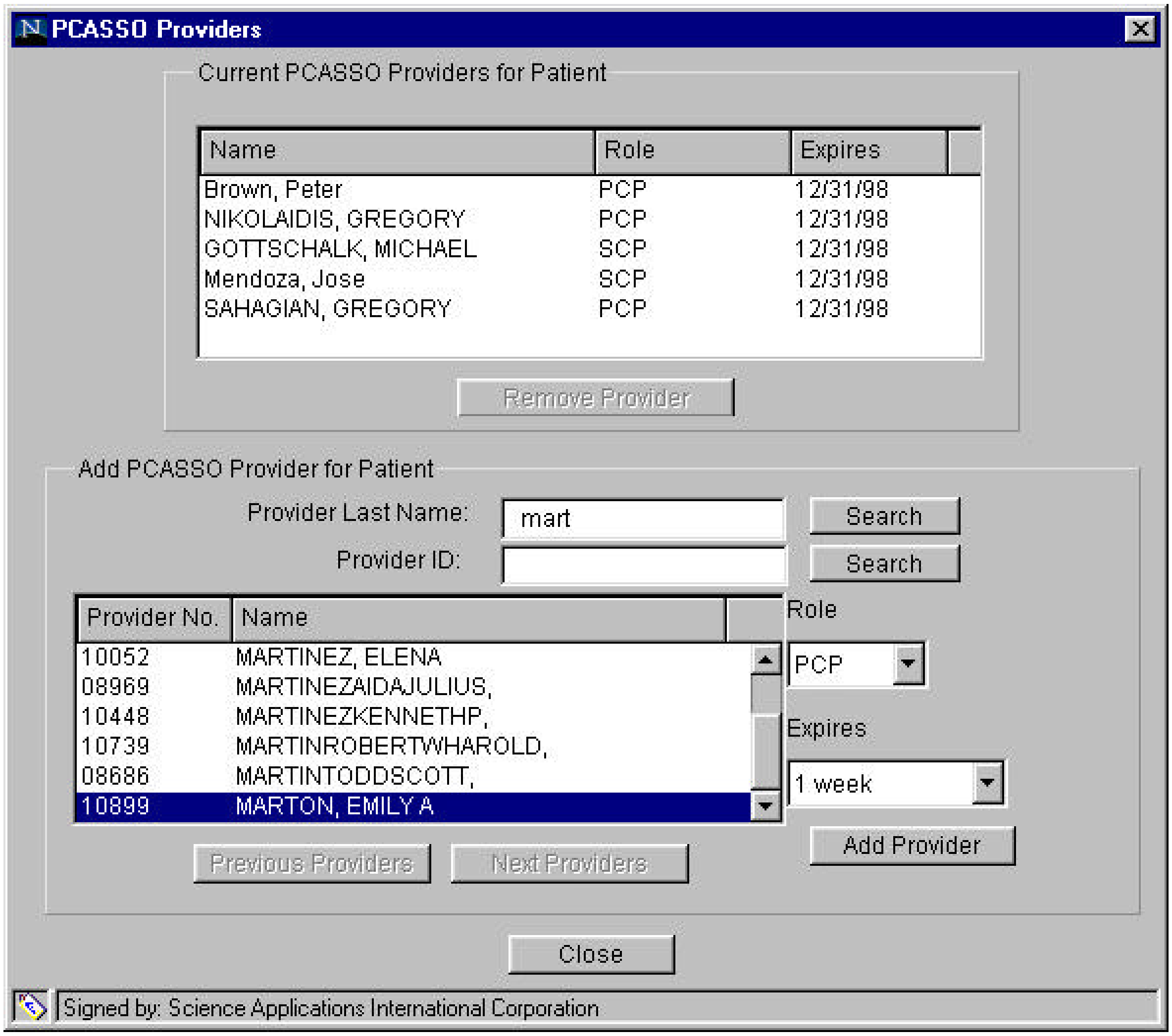
"Access Matrix": Three objects and five subjects are depicted in this matrix.

role-based access control adds hierarchies of roles and information to access matrix

Role	**Access**
Patient	all information for the patient
Doctor	all information
Voluntary caring agency	name, address, clinical data
Researcher	age, sex, clinical data
Organization staff	name and ID

Table “Example Role and Access”

PCASSO (http://medicine.ucsd.edu/pcasso)



Current PCASSO Providers for Patient

Name	Role	Expires
Brown, Peter	PCP	12/31/98
NIKOLAIDIS, GREGORY	PCP	12/31/98
GOTTSCHALK, MICHAEL	SCP	12/31/98
Mendoza, Jose	SCP	12/31/98
SAHAGIAN, GREGORY	PCP	12/31/98

Add PCASSO Provider for Patient

Provider Last Name: mart

Provider ID:

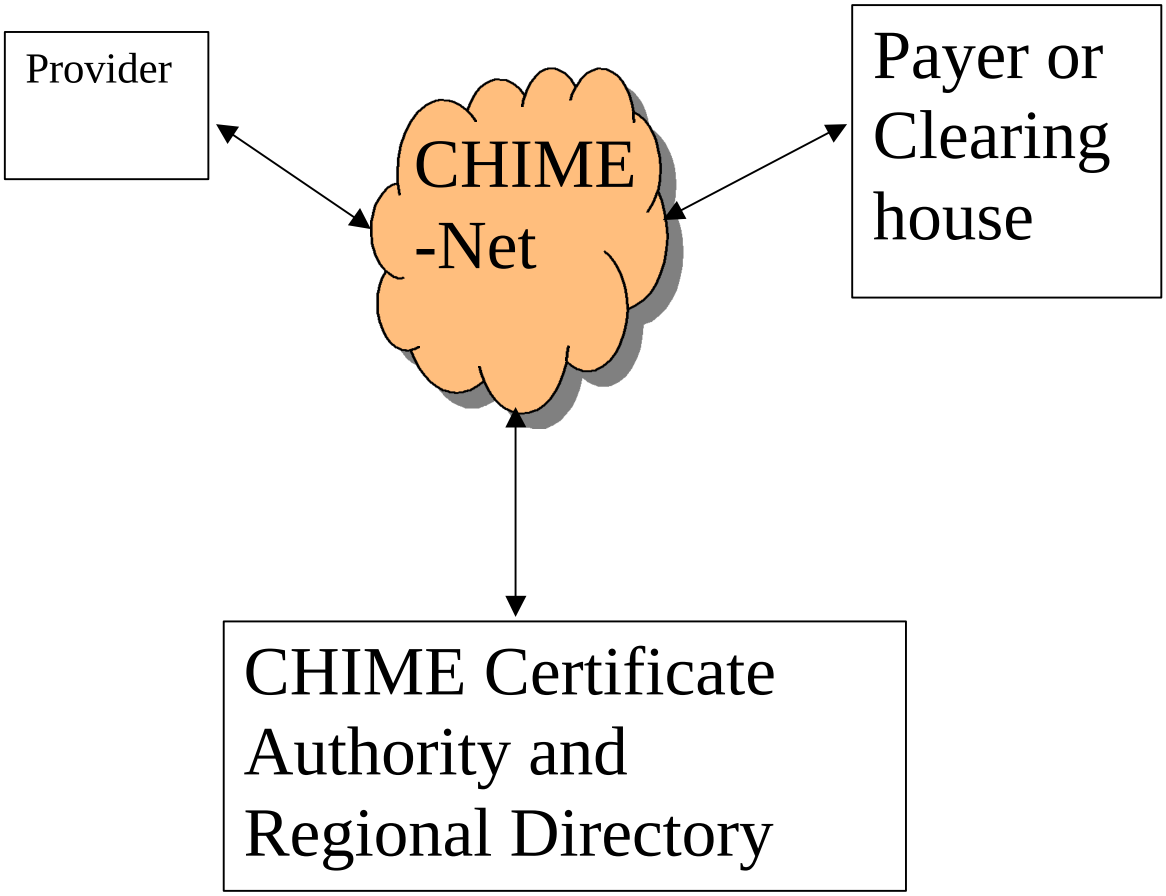
Provider No.	Name
10052	MARTINEZ, ELENA
08969	MARTINEZAIDAJULIUS,
10448	MARTINEZKENNETHP,
10739	MARTINROBERTWHAROLD,
08686	MARTINTODDSCOTT,
10899	MARTON, EMILY A

Role: PCP

Expires: 1 week

Signed by: Science Applications International Corporation

6.3 Technical Mechanism



PKI uses PK and requires workflow management for keys.

7 Conclusion

7.1 Summary

Transaction Rule provides part of the common language.

Privacy rule and Security Proposed Rule give decision guides.

‘Minimum necessary use’ requires that people be grouped into roles and that those roles are related to certain actions on certain categories of information.

Security:

- policies such as from Kaiser indicate the organizational approach,
- computer models like role-based access are part of workflow systems,
- mechanisms such as PKI require again organizational models.

Privacy and security are less about stopping people from doing things than about making sure that the right people do the right thing.

Relate to ISO 9000 (www.iso.ch) quality management.

Mapping Documents and Behavior			
		documents relative to standard	
		good	**bad**
behavior relative to documents	**good**	documents conform to standard and people follow documents	documents do not follow standards but people follow documents
	bad	documents conform to standard but people do not	documents do not follow the standard or are missing and people do not follow them

7.2 Where Next?

Coordination Language: Need standardized medical record. HIPAA has initiated (http://www.ncvhs.hhs.gov/).

Need workflow models.

Privacy Rule calls for associations to provide these for their members.

Privacy Rule encourages the sharing of:

- defining and mapping roles to categories of information
- forms such as authorization forms and privacy notices

Such generic tools will reduce costs.

HIMSS HIPAA SIG would like to help collect (flex.ifsm.umbc.edu/HIPAA).

Are you willing to share any?

HIPAA Summit invited me to offer my book *HIPAA@IT*. Few copies available here!