Hybrid Policies

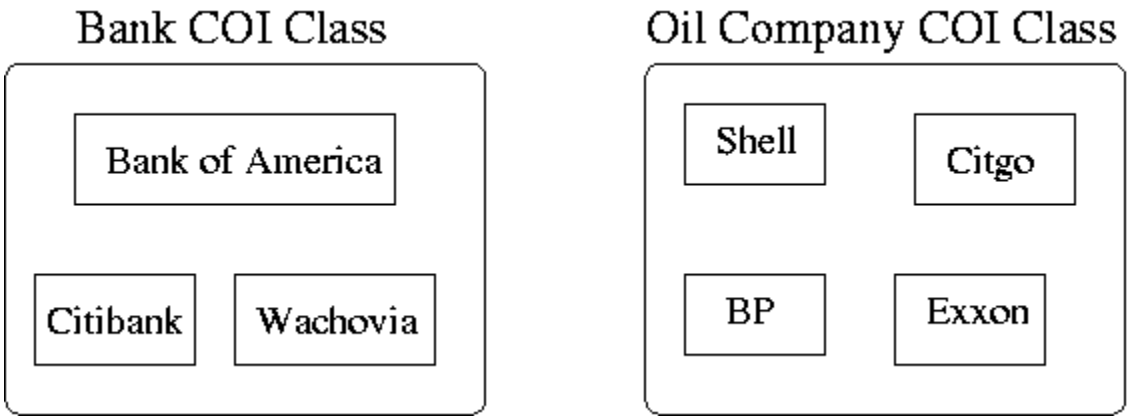
Chinese Wall Model

Security policy that refers equally to confidentiality and integrity
Describes policies that involve conflict of interest in business

Def: The objects of the database are items of information related to a company

Def: A Company Dataset (CD) contains objects related to a single company

Def: A Conflict Of Interest (COI) class contains the datasets of companies in competition



CW-Simple Security Condition

S can read O iff either

1. There is an object O such that S has accessed O' and CD(O') = CD(O)

or

2. For all objects O', O' $\in$ PR(S) $\Rightarrow$ COI(O') $\neq$ COI(O) where PR(S) is the set of previously read objects by S.

Subject affects:

a. Once a subject reads any object in a COI class, the only other objects that the subject can read in that class are the same objects, i.e. once one object is read, no other objects in another class can be read.

b. The minimum number of subjects needed to access each object in a class is the number of objects in that class.

Since most companies have information that is available to all subjects, the model distinguishes between sanitized and unsantized data by adding condition 3,

3. O is a sanitized object.

The complete CW-Simple Security Condition is

CW-Simple Security Condition

S can read O iff either

1. There is an object O such that S has accessed O' and CD(O') = CD(O)
2. For all objects O', O' $\in$ PR(S) $\Rightarrow$ COI(O') $\neq$ COI(O) where PR(S) is the set of previously read objects by S.
3. O is a sanitized object.

Since two subjects could have access to the same object in one COI and different objects in another COI, we have

CW-*-Property

A subject S may write to an object O iff both of the following conditions hold

1. The CW-Simple security conditions permits S to read O
2. $\forall$ unsantized objects O', S can read O' $\Rightarrow$ CD(O') = CD(O)

This prevents one subject from writing sensitive information in the shared common object from an unshared object.

Clinical Information Systems Security Policy

Electronic medical records present their own requirements for policies that combine confidentiality and integrity. Patient confidentiality, authentication of both records and those making entries in those records, and assurance that the records have not been changed erroneously are most critical.

Def: A *patient* is the subject of medical records, or an agent for that person who can give consent for the person to be treated.

Def: *Personal health information* (electronic medical record) is information about a patient's health or treatment enabling that patient to be identified.

Def: A *clinician* is a health-care professional who has access to personal health information while performing his or her job.

Guided by the Clark-Wilson model, we have a set of principles that address electronic medical records.

Access to the electronic medical records must be restricted to the clinician and the clinician's practice group.

Access Principle 1: Each medical record has an access control list naming the individuals or groups who may read and append information to the record. The system must restrict access to those identified on the access control list.

Medical ethics require that only clinicians and the patient have access to the patient's electronic medical records.

Access Principle 2: One of the clinicians on the access control list (called the responsible clinician) must have the right to add other clinicians to the access control list.

The patient must consent to any treatment. Hence, the patient has the right to know when his or her electronic medical records are accessed or altered. Also the electronic medical records system must prevent the leakage of information. Hence, the patient must be notified when their electronic medical records are accessed by a clinician that the patient does not know.

Access Principle 3: The responsible clinician must notify the patient of the names on the access control list whenever the patient's medical record is opened. Except in situations given in statutes or in cases of emergency, the responsible clinician must obtain the patient's consent.

Auditing who accesses the patient's electronic medical records, when those records were accessed, and what changes, if any, were made to the electronic medical records must be recorded to adhere to numerous government medical information requirements.

Access Principle 4: The name of the clinician, the date, and the time of the access of a medical record must be recorded. Similar information must be kept for deletions.

The following principles deal with record creation, and information deletion. New electronic medical records should allow the attending clinician and the patient access to those records. Additionally, the referring clinician, if any, should have access to those records to see the results of any referral.

Creation Principle: A clinician may open a record, with the clinician and the patient on the access control list. If the record is opened as a result of a referral, the referring clinician may also be on the access control list.

Electronic medical records should be kept the required amount of time, normally 8 years except in some instances.

Deletion Principle: Clinical information cannot be deleted from a medical record until the appropriate time has passed.

When copying electronic medical records, care must be taken to prevent the unauthorized disclosure of a patient's medical records.

Confinement Principle: Information from one medical record may be appended to a different medical record if and only if the access control list of the second record is a subset of the access control list of the first.

The combining of information from numerous authorized sources may lead to new information that the clinician should not have access to. Also the access to a wide set of medical records would make the individual clinician susceptible to corruption or blackmail.

Aggregation Principle: Measures for preventing the aggregation of patient data must be effective. In particular a patient must be notified if anyone is to be added to the access control list for the patient's record and if that person has access to a large number of medical records.

There must be system mechanisms implemented to enforce all of these principles.

Enforcement Principle: Any computer system that handles medical records must have a subsystem that enforces the preceding principles. The effectiveness of this enforcement must be subject to evaluation by independent auditors.