Privacy Engineering (408)

Privacy Policies

Exercises

Write S4P specifications for the following hospital patient record system.

Label your S4P assertions and queries. Underline S4P keywords *says*, *may*, *will*, *can say*, *exists*.

State any assumptions that you make, e.g. due to missing or ambiguous wording.

1. **Imperial Hospital Privacy Policy**

   (i) Doctors of the hospital are permitted to access the records of patients under their care. Any doctor is permitted to access the record of a patient they treat in a medical emergency – however an audit of the access will be carried out within 3 days.

   (ii) Doctors are able to delegate access to their patient's record to a nurse of the hospital.

   (iii) Doctors must be registered with the British Medical Association (BMA). Nurses must be registered with the Nursing and Midwifery Council (NMC).

   (iv) Doctors cannot be nurses.

   (v) Doctors and nurses cannot access their own record.

2. **Patient Pat's Privacy Preferences**

   (i) Doctors and nurses of a hospital can access Pat's hospital record if Pat is a patient at that hospital and he gives his consent.

   (ii) If Pat is unable to give consent, for example, if Pat is unconscious, then consent can be given by his next of kin, Mary.

   (iii) In an emergency, any doctor treating Pat can access Pat's patient record, but accesses must be subject to a follow up audit within 7 days.

3. How would we check that Imperial's privacy policy (question 1) would be satisfied by Pat's privacy preferences (question 2)?

   Which assertions would need to be satisfied to enable nurse Nancy to access Pat's record? You can add new assertions for Principals.