Privacy Engineering (408)

Privacy Policies

Solutions

1(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.
Will Promise	Ia1	Imperial says D will access(D, Record(P)) if patient(P, Imperial), doctor(D, Imperial), care(D, P) where D != P // to handle 1(v)
Will Promise	Ia2	Imperial says D will access(D, Record(P)) if emergency(P), doctor(D, Imperial), patient(P, Imperial)
Will Promise	Ia3	Imperial says Imperial will audit(Record(P),3 days) if emergency(P), *accessed*(D, record(P))
May query	Iq1	P says Imperial may access(D, Record(P)) ?

1(ii)		Doctors are able to delegate access to their patients record to a nurse of the hospital.
Delegation	Ia4	Imperial says D can say access(N, Record(P)) if access(D, record(P)), doctor(D, Imperial), nurse(N, Imperial) where N != P // to handle 1(v)

1(iii)		Doctors must be registered with the British Medical Association (BMA). Nurses must be registered with the Nursing and Midwifery Council (NMC).
Delegation	Ia5	Imperial says BMA can say doctor(D) if registered(D, BMA)
Delegation	Ia6	Imperial says NMC can say nurse(N) if registered(N, NMC)

1(iv)		Doctors cannot be nurses.
Promise	Ia7	Imperial says D != N if doctor(D, Imperial), nurse(N, Imperial)

1(v)		Doctors and nurses cannot access their own record.
		See ia1 and ia4

2(i)		Doctors and nurses of a hospital can access Pats hospital record if Pat is a patient at that hospital and he gives his consent.
May Permission	Pa1	Pat says DN may access(DN, Record(Pat)) if patient(Pat, H), doctor_or_nurse(DN, H)

2(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.
Delegation	Pa2	Pat says Mary can say access(DN, Record(Pat) if unable(Pat)

2(iii)		In an emergency, any doctor treating Pat can access Pats patient record, but accesses must be subject to a follow up audit within 7 days.
May Permission	Pa3	Pat says H may access(D, Record(Pat)) if emergency(Pat)
Will Query	Pq1	exists t: H says H will audit(Record(Pat), t)?, t <= 7 days?, emergency(Pat), *accessed*(D, Pat)

3		How would we check that Imperial's privacy policy (question 1) would be satisfied by Pat's privacy preferences (question 2)?
		For policy satisfaction, we need to check Pat's ***will*** query (Pq1) and Imperial's ***may*** (Iq1) query against the union of Pat's and Imperial's assertions.
		Which assertions would need to be satisfied to enable nurse Nancy to access Pat's record? You can add new assertions for Principals.
		From Imperial's policies, for some Doctor e.g. David: Imperial says David can say access(Nancy, Record(Pat)) if access(David, record(Pat)), doctor(David, Imperial), nurse(Nancy, Imperial) where Nancy != Pat Imperial says David will access(David, Record(Pat)) if patient(Pat, Imperial), doctor(David, Imperial), care(David, Pat) where David != Pat Imperial says David != Nancy if doctor(David, Imperial), nurse(Nancy, Imperial) Imperial says BMA can say doctor(David) if registered(David, BMA) Imperial says NMC can say nurse(Nancy) if registered(Nancy, NMC) From Pat's preferences either Pa1 or Pa2: Pat says Nancy may access(Nancy, Record(Pat) if patient(Pat, Imperial), doctor_or_nurse(Nurse, Imperial) or Pat says Mary says access access(Nanacy, Record(Pat) if unable(Pat0) Plus new assertions: Imperial **says** patient(Pat, Imperial) Imperial says doctor(David, Imperial) Imperial says nurse(Nurse, Imperial) Imperial **says** care(David, Pat) BMA **says** registered(David, BMA) NMC **says** registered(Nancy, NMC)